

SDX 10.1

Apr 12, 2016

[Release Notes](#)

[Hardware Installation](#)

[NetScaler SDX Hardware and Component Compatibility Matrix](#)

[Getting Started with the Management Service and User Interface](#)

[Hardware Installation](#)

[Common Hardware Components](#)

[Field Replaceable Units](#)

[Hardware Platforms](#)

[Summary of Hardware Specifications](#)

[Preparing for Installation](#)

[Installing the Hardware](#)

[Initial Configuration](#)

[Lights Out Management Port of the NetScaler SDX Appliance](#)

[Upgrading the Components of a NetScaler SDX Appliance](#)

[Upgrading the Management Service](#)

[Upgrading the XenServer Software](#)

[Uploading and Applying a XenServer Hotfix](#)

[Installing the XenServer Supplemental Pack](#)

[Upgrading a NetScaler Instance](#)

[Managing and Monitoring the NetScaler SDX Appliance](#)

[Managing the RAID disk allocation](#)

[NetScaler SDX Licensing Overview](#)

[Managing Interfaces](#)

[Configuring SNMP on NetScaler SDX Appliances](#)

[Configuring Syslog Notifications](#)

[Configuring Mail Notifications](#)

[Configuring SMS Notifications](#)

[Monitoring and Managing the Real-Time Status of Entities Configured on NetScaler Devices](#)

[Monitoring and Managing Events Generated on NetScaler Instances](#)

[Call Home Support for NetScaler Instances on NetScaler SDX](#)

[System Health Monitoring](#)

[Configuring the Management Service](#)

[Configuring Authentication and Authorization Settings](#)

[Configuring the External Authentication Server](#)

[Configuring Link Aggregation from the Management Service](#)

[Configuring a Channel from the Management Service](#)

[Backing Up and Restoring the Configuration Data of the SDX Appliance](#)

[Performing a Factory Reset](#)

[Provisioning NetScaler Instances](#)

[Setting up a Cluster of NetScaler Instances](#)

[Configuring and Managing NetScaler Instances](#)

[Configuring Authentication and Authorization Settings](#)

[Configuring the External Authentication Server](#)

[Configuring Link Aggregation from the Management Service](#)

[Configuring a Channel from the Management Service](#)

[Backing Up and Restoring the Configuration Data of the SDX Appliance](#)

[Performing a Factory Reset](#)

[Monitoring NetScaler Instances](#)

[Using Logs to Monitor Operations and Events](#)

[Use Cases for NetScaler SDX Appliances](#)

[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](#)

[Consolidation Across Security Zones](#)

[Converting a NetScaler MPX Appliance to a NetScaler SDX Appliance](#)

[Converting a NetScaler MPX 11515/11520/11530/11540/11542 Appliance to a NetScaler SDX 11515/11520/11530/11540/11542 Appliance](#)

[Converting a NetScaler MPX 8200/8400/8600/8800 Appliance to a NetScaler SDX 8400/8600 Appliance](#)

[Converting a NetScaler MPX 14020/14030/14040/ 14060/14080/14100 Appliance to a NetScaler SDX 14020/14030/14040/ 14060/14080/14100 Appliance](#)

[Converting a NetScaler MPX 24100 and 24150 Appliance to a NetScaler SDX 24100 and 24150 Appliance](#)

Third-Party Virtual Machines

[SECUREMATRIX GSB](#)

[Websense Protector](#)

[BlueCat DNS/DHCP](#)

[CA Access Gateway](#)

[Palo Alto Networks VM-Series](#)

Nitro API

[Obtaining the NITRO Package](#)

[How NITRO Works](#)

[Java SDK](#)

[.NET SDK](#)

[REST Web Services](#)

Release Notes

Dec 31, 2013

Release notes describe the enhancements, changes, bug fixes, and known issues for a particular release or build of Citrix NetScaler software. The NetScaler SDX release notes are covered as a part of NetScaler release notes.

For detailed information about SDX 10.1 enhancements, known issues, and bug fixes, see: [NetScaler 10.1](#)

Hardware Installation

Apr 08, 2015

All NetScaler SDX appliances share common components, but different platforms have different additional components. Therefore, installation requirements can vary among platforms. Before installation, make sure that your site is suitable for your appliance and that you have completed all necessary preparations. This is also the time to read the cautions and warnings. You are then ready to mount the appliance in a rack, connect it, and start it up. For initial configuration, you can connect a computer to the appliance's network or to its serial-console port. After initial configuration, you can configure the Lights Out Management port, so that you have management access to the appliance even if your network goes down.

The Citrix NetScaler SDX appliance is a multi-tenant platform on which you can provision and manage multiple virtual instances of NetScaler.

The Citrix NetScaler SDX product line consists of:

- Citrix NetScaler SDX 8015/8400/8600
- Citrix Netscaler SDX 11500/13500/14500/16500/18500/20500
- Citrix Netscaler SDX 11515/11520/11530/11540/11542
- Citrix Netscaler SDX 17500/19500/21500
- Citrix Netscaler SDX 17550/19550/20550/21550
- Citrix Netscaler SDX 22040/22060/22080/22100/22120
- Citrix Netscaler SDX 24100/24150

NetScaler SDX Hardware and Component Compatibility Matrix

Sep 02, 2014

Points to note

Before you decide to upgrade any component of NetScaler SDX, make sure to refer the following points:

- Some NetScaler SDX features have minimum version requirements across various NetScaler SDX components. Refer table 2 for detailed information.
- Any combinations of Management Service and NetScaler versions are supported as long as they meet minimum version requirements for a particular hardware platform.
 1. Refer Table 1 for NetScaler SDX hardware, Management Service and NetScaler version compatibility.
 2. Refer table 2 for specific feature-component compatibility.
- A NetScaler SDX appliance is always shipped with a validated and tested release bundle (that includes a specific combination of Management Service, XenServer and XS Supplemental Pack versions), and will work out of the box. It is advised that users looking to upgrade any of these components upgrade to an appropriate release bundle as recommended on the Citrix download page"
- XenServer and supplement packs should be upgraded based on a feature's requirement, else they should be kept as those shipped from the factory. Refer table 2 to understand the feature-component compatibility information. If you need to upgrade XenServer and supplemental packs, then you must download the images for XenServer and supplemental packs from the Citrix NetScaler SDX Download page.
- Make sure to check the Citrix NetScaler SDX download page for the recommended hot fixes applicable for the Management Service version.

The following table lists the compatible NetScaler and Management Service versions for NetScaler SDX platform:

Table 1. NetScaler and Management Service Versions for NetScaler SDX Platform

NetScaler SDX Platform	Management Service Version	NetScaler Version
SDX 17500/19500/21500	Supported <ol style="list-style-type: none"> 1. Release 9.3 build 48.6 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later 	Supported <ol style="list-style-type: none"> 1. Release 9.3 build 48.6 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later
SDX 11500/13500/14500/16500/18500/20500	Supported <ol style="list-style-type: none"> 1. Release 9.3 build 49.5 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later 	Supported <ol style="list-style-type: none"> 1. Release 9.3 build 49.5 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later
SDX 17550/19550/20550/21550	Supported	Supported

NetScaler SDX Platform	Management Service Version	NetScaler Version
	<ol style="list-style-type: none"> 1. Release 9.3 build 52.3 and later 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later 	<ol style="list-style-type: none"> 1. Release 9.3 build 52.3 and later 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later
SDX 11500/13500/14500/16500/18500/20500 NEBS	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 9.3 build 61.5 and later 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later 	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 9.3 build 61.5 and later 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later
SDX 8400/8600	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 10.0 build 74.4 and later 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later 	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 10.0 build 74.4 and later 2. Release 10.1 build 118.7 and later 3. Release 10.5 build 50.10 and later
SDX* 22040/22060/22080/22100	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 10.1 build 123.11 and later 2. Release 10.5 build 50.10 and later <p>Not Supported</p> <ul style="list-style-type: none"> • Release 9.3 	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 10.1 build 123.11 and later 2. Release 10.5 build 50.10 and later <p>Not Supported</p> <ul style="list-style-type: none"> • Release 9.3
SDX 8015	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 10.1, build 123.11 and later 2. Release 10.5 build 52.11 and later <p>Not Supported</p> <ul style="list-style-type: none"> • Release 9.3 	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 10.1, build 123.11 and later 2. Release 10.5 build 52.11 and later <p>Not Supported</p> <ul style="list-style-type: none"> • Release 9.3
SDX 11515/11520/11530/11540/11542	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 10.1, build 124.13 and later 2. Release 10.5 build 50.10 and later 	<p>Supported</p> <ol style="list-style-type: none"> 1. Release 10.1, build 124.13 and later 2. Release 10.5 build 50.10 and later

NetScaler SDX Platform	Not Supported Management Service Version • Release 9.3	Not Supported NetScaler Version • Release 9.3
SDX 24100/24150	Supported 1. Release 10.1, build 129.11 and later 2. Release 10.5 build 51.10 and later Not Supported • Release 9.3	Supported 1. Release 10.1, build 129.11 and later 2. Release 10.5 build 51.10 and later Not Supported • Release 9.3

*SDX 22040/22060/22080/22100 platforms require XenServer supplemental pack 100013 and higher.

The following table lists the compatible NetScaler SDX components and feature compatibility. Component implies Management Service, NetScaler, XenServer and XenServer Supplemental Pack versions.

Table 2. NetScaler SDX Features and Components Compatibility

SDX Feature	Management Service Version	NetScaler Version	XenServer Version	SDX Supplemental Pack Version
LACP as shared resource	Supported 1. Release 10.1, build 118.7 and later 2. Release 10.5 build 50.10 and later Not Supported • Release 9.3	Supported 1. Release 10.1, build 118.7 and later 2. Release 10.5 build 50.10 and later Not Supported • Release 9.3	Release 6.1 and later	NA
VLAN Whitelist	Supported 1. Release 10.1, build 118.7 and later 2. Release 10.5 build 50.10 and later Not Supported • Release 9.3	Supported 1. Release 10.1, build 118.7 and later 2. Release 10.5 build 50.10 and later Not Supported • Release 9.3	Release 6.0 and later	Build 100007 and higher
Palo Alto Guest VM	Supported 1. Release 10.5 build 50.10 and later Not Supported • Release 9.3	NA	Release 6.1 and later	Build 100012 and higher

SDX Feature	Support Service Version	NetScaler Version	XenServer Version	SDX Supplemental Pack Version
MAC	<p>Supported</p> <ul style="list-style-type: none"> 1. Release 10.1 build 118.7 and later 2. Release 10.5 build 50.10 and later <p>Not Supported</p> <ul style="list-style-type: none"> 1. Release 9.3 	<p>Supported</p> <ul style="list-style-type: none"> 1. Release 10.1 build 118.7 and later 2. Release 10.5 build 50.10 and later <p>Not Supported</p> <ul style="list-style-type: none"> 1. Release 9.3 		
NetScaler Cluster on SDX	<p>Supported</p> <ul style="list-style-type: none"> 1. Release 10.1 build 118.7 and later 2. Release 10.5 build 50.10 and later <p>Not Supported</p> <ul style="list-style-type: none"> 1. Release 9.3 	<p>Supported</p> <ul style="list-style-type: none"> 1. Release 10.1 build 118.7 and later 2. Release 10.5 build 50.10 and later <p>Not Supported</p> <ul style="list-style-type: none"> 1. Release 9.3 	Version 6.0 and later	100007 and higher

Getting Started with the Management Service User Interface

Jan 31, 2011

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:
 1. 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.
 2. 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.

Initial Setup Wizard

You can use the Setup Wizard to complete all the first time configurations in a single flow.

You can use the wizard to configure network configuration details and system settings, change the default administrative password, and manage and update licenses.

You can also use this wizard to modify the network configuration details that you specified for the NetScaler SDX

appliance during initial configuration.

To access the wizard, navigate to Configuration > System and, under Set Up Appliance, click Setup Wizard.

On the Platform Configuration page, you can configure network configuration details, system settings, and change the default administrative password.

- Interface*—The interface through which clients connect to the Management Service. Possible values: 0/1, 0/2. Default: 0/1.
- XenServer IP Address*—IP address of the XenServer server.
- Management Service IP Address*—IP address of the Management Service.
- Netmask*—Mask for the subnet in which the SDX appliance is located.
- Gateway*—Default gateway for the network.
- DNS Server—IP address of the DNS server.

Under System Settings, you can specify that the Management Service and a NetScaler 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.

You can modify the time zone of the Management Service and the XenServer server. The default time zone is UTC. You can change the Administrative password by selecting the Change Password check box and typing the new password.

Under Manage Licenses you can manage and allocate licenses. You can use your hardware serial number (HSN) or your license activation code (LAC) to allocate your licenses. Alternatively, if a license is already present on your local computer, you can upload it to the appliance.

Select the licenses on the appliance and click Done to complete the initial configuration.

Provisioning Instances on an SDX Appliance

You can provision one or more NetScaler or third-party 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 third-party instances, see [Third-Party Virtual Machines](#).

Console Access

You can access the console of NetScaler instances, the Management Service, XenServer, and third party VMs from the Management Service interface. This is particularly helpful in debugging and troubleshooting the instances hosted on the NetScaler SDX appliance.

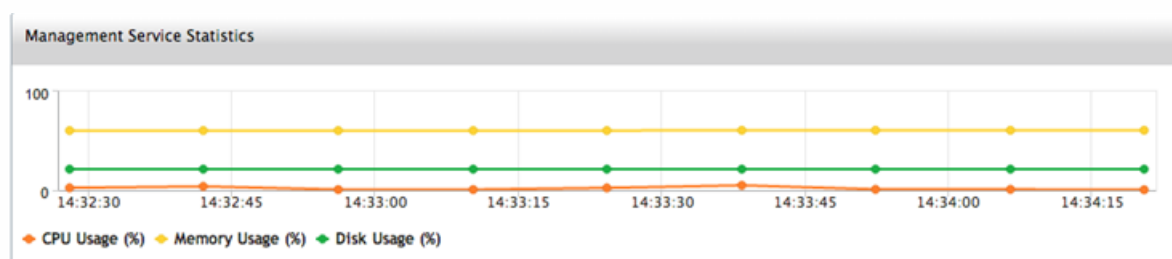
To access the console of VMs, navigate to the instance listing, select the VM from the list, and under Action drop down menu, click Console Access.

To access the console of Management Service or XenServer, navigate to Configuration > System, and under Console Access, click Management Service or XenServer link.

Note: Console access is not supported by the Internet Explorer browser. Citrix recommends using the console access feature through Management Service HTTPS sessions only.

Management Service Statistics

The dashboard now includes Management Service Statistics for monitoring use of memory, CPU, and disk resources by the Management Service on NetScaler SDX appliance.



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 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 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.

Hardware Installation

Apr 08, 2015

All NetScaler SDX appliances share common components, but different platforms have different additional components. Therefore, installation requirements can vary among platforms. Before installation, make sure that your site is suitable for your appliance and that you have completed all necessary preparations. This is also the time to read the cautions and warnings. You are then ready to mount the appliance in a rack, connect it, and start it up. For initial configuration, you can connect a computer to the appliance's network or to its serial-console port. After initial configuration, you can configure the Lights Out Management port, so that you have management access to the appliance even if your network goes down.

The Citrix NetScaler SDX appliance is a multi-tenant platform on which you can provision and manage multiple virtual instances of NetScaler.

The Citrix NetScaler SDX product line consists of:

- Citrix NetScaler SDX 8015/8400/8600
- Citrix Netscaler SDX 11500/13500/14500/16500/18500/20500
- Citrix Netscaler SDX 11515/11520/11530/11540/11542
- Citrix Netscaler SDX 17500/19500/21500
- Citrix Netscaler SDX 17550/19550/20550/21550
- Citrix Netscaler SDX 22040/22060/22080/22100/22120
- Citrix Netscaler SDX 24100/24150

Common Hardware Components

Jan 28, 2011

Each platform has front panel and back panel hardware components. The front panel has an LCD display and an RS232 serial console port. The number, type, and location of ports—copper Ethernet, copper and fiber 1G SFP, and 10G SFP+—vary by hardware platform. The back panel provides access to the fan and the field replaceable units (power supplies, CompactFlash card, and solid-state and hard-disk drives).

LCD Display and LED Status Indicators

On some NetScaler SDX appliances, the LCD on the front panel displays the appliance's model number, but the number shown might not be the licensed model number. To view the licensed model number of any SDX appliance, log on to the Management Service and check the licensed model number in the top left corner of the screen. For example, if you have purchased an SDX 11515 license, the LCD screen displays CITRIX NSSDX-11500, and the Management Service screen displays NetScaler SDX (11515).

The LCD backlight on the NetScaler SDX 22040/22060/22080/22100/22120 is always on. For all other SDX appliances, the LCD backlight lights up only when the appliance is restarted or powered on. The backlight on these appliances remains on for some time and automatically turns off.

On the appliance's back panel, system status LEDs indicate the overall status of the appliance. The following table describes the indicators of the system status LED.

Note: System status LEDs are available on only the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 appliances.

LED Color	LED Indicates
OFF	No power
Green	Appliance is receiving power
Red	Appliance has detected an error

On the appliance's back panel, power status LEDs indicate the status of each power supply. The following table describes the indicators of the power status LED.

LED Color	LED Indicates
OFF	No power
Green	Appliance is receiving power
Red	Power supply has detected an error

The port LEDs show whether a link is established and traffic is flowing through the port. The following table describes the LED indicators for each port. There are two LED indicators for each port type.

Table 1. LED port-status indicators

Port Type	LED Location	LED Function	LED Color	LED Indicates
10G SFP+ (10 Gbps)	Top	Speed	Off	No connection.
			Solid blue	Traffic rate of 10 gigabits per second.
	Bottom	Link/ Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the port.
			Blinking green	Traffic is passing through the port.
	1G SFP (1 Gbps)	Left	Link/ Activity	Off
Solid green				Link is established but no traffic is passing through the port.
Blinking green				Traffic is passing through the port.
Right		Speed	Off	No connection.
			Yellow	Traffic rate of 1 gigabit per second.
Ethernet (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.
			Yellow	Traffic rate of 1 gigabit per second.
	Right	Link/ Activity	Off	No link.
			Solid green	Link is established but no traffic is passing through the port.
			Blinking	Traffic is passing through the port.

Port Type	LED Location	LED Function	LED Color	LED Indicates
Management (RJ45)			Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.
			Amber	Traffic rate of 1 gigabit per second.
	Right	Link/ Activity	Off	No link.
			Solid yellow	Link is established but no traffic is passing through the port.
			Blinking yellow	Traffic is passing through the port.

On each power supply, a bicolor LED indicator shows the condition of the power supply.

Table 2. LED Power Supply Indicators

Power Supply Type	LED Color	LED Indicates
AC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing GREEN	Power supply is in standby mode.
	GREEN	Power supply is functional.
	RED	Power supply failure.
DC	OFF	No power to any power supply.
	Flashing RED	No power to this power supply.
	Flashing BLUE	Power supply is in standby mode.
	BLUE	Power supply is functional.
	RED	Power supply failure.

Ports

Ports are used to connect the appliance to external devices. NetScaler appliances support RS232 serial ports, 10/100/1000Base-T copper Ethernet ports, 1-gigabit copper and fiber 1G SFP ports, and 10-gigabit fiber SFP+ ports. All NetScaler appliances have a combination of some or all of these ports. For details on the type and number of ports available on your appliance, see the section describing that platform.

RS232 Serial Port

The RS232 serial console port provides a connection between the appliance and a computer, allowing direct access to the appliance for initial configuration or troubleshooting.

All hardware platforms ship with an appropriate serial cable used to connect your computer to the appliance. For instructions on connecting your computer to the appliance, see "[Installing the Hardware](#)."

Copper Ethernet Ports

The copper Ethernet ports installed on many models of the appliance are standard RJ45 ports.

There are two types of copper Ethernet ports that may be installed on your appliance:

10/100BASE-T port

The 10/100BASE-T port has a maximum transmission speed of 100 megabits per second (Mbps). Most platforms have at least one 10/100BASE-T port.

10/100/1000BASE-T port

The 10/100/1000BASE-T port has a maximum transmission speed of 1 gigabit per second, ten times faster than the other type of copper Ethernet port. Most platforms have at least one 10/100/1000Base-T port.

To connect any of these ports to your network, you plug one end of a standard Ethernet cable into the port and plug the other end into the appropriate network connector.

Management Ports

Management ports are standard copper Ethernet ports (RJ45), which are used for direct access to the appliance for system administration functions.

1G SFP and 10G SFP+ Ports

A 1G SFP port can operate at a speed of 1 Gbps. It accepts either a copper 1G SFP transceiver, for operation as a copper Ethernet port, or a fiber 1G SFP transceiver for operation as a fiber optic port.

The 10G SFP+ ports are high-speed ports that can operate at speeds of up to 10 Gbps. You need a fiber optic cable to connect to a 10G SFP+ port. If the other end of the fiber optic cable is attached to a 1G SFP port, the 10G SFP+ port automatically negotiates to match the speed of the 1G SFP port.

Ports Compatibility

The 10G slot supports **copper** 1G transceivers, which can operate at up to 1 Gbps in a 10 Gbps slot.

Note: You cannot insert a fiber 1G transceiver into a 10G slot.

Note: You cannot insert a 10G transceiver into a 1G slot.

1G Pluggable Media

The following table lists the maximum distance specifications for 1G transceivers.

Table 3. Copper 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Cable Type	Typical Reach (m)	Products
EW3A0000235, EW3B0000235, EW3C0000235, EW3D0000235, EW3E0000235, EW3F0000235, EW3P0000143, EW3X0000235, EW3Z0000087	Citrix NetScaler 1G SFP Ethernet Copper (100m) - 4 Pack	n/a	Category 5 (Cat-5) Copper Cable	100 m	SDX 8015/8400/8600, SDX 22040/22060/22080/22100/22120, SDX 24100/24150

Table 4. Short Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000234, EW3B0000234, EW3C0000234, EW3D0000234, EW3E0000234, EW3F0000234, EW3P0000142, EW3X0000234, EW3Z0000086	Citrix NetScaler 1G SFP Ethernet SX (300m) - 4 Pack	850nm (nominal)	50/125um MMF, 2000MHz-km (OM3)	550 m	SDX 8015/8400/8600, SDX 22040/22060/22080/22100/22120, SDX 24100/24150
			50/125um MMF, 500MHz-km (OM2)	550 m	
			50/125um MMF, 400MHz-km	550 m	
			62.5/125um MMF, 200MHz-km (OM1)	300 m	
			62.5/125um MMF, 160MHz-km	300 m	

Table 5. Short Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000710, EW3B0000710, EW3C0000710, EW3D0000710, EW3E0000710, EW3F0000710, EW3P0000557, EW3X0000710, EW3Z0000585	Citrix NetScaler 1G SFP Ethernet Short Range (300m) - Single	850nm (nominal)	50/125um MMF, 2000MHz-km (OM3)	550 m	SDX 8015/8400/8600, SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, SDX 17500/19500/21500, SDX 22040/22060/22080/22100/22120, SDX 24100/24150
			50/125um MMF, 500MHz-km (OM2)	550 m	
			50/125um MMF, 400MHz-km	550 m	
			62.5/125um MMF, 200MHz-km (OM1)	275 m	
			62.5/125um MMF, 160MHz-km	220 m	

Table 6. Long Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000712, EW3B0000712, EW3C0000712, EW3D0000712, EW3E0000712, EW3F0000712, EW3P0000559, EW3X0000712, EW3Z0000587	Citrix NetScaler 1G SFP Ethernet LX - Single	1310nm (nominal)	9/125um SMF	10 km	SDX 8015/8400/8600, SDX 22040/22060/22080/22100/22120, SDX 24100/24150

Table 7. Long Reach Fiber 1G SFP Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000711, EW3B0000711, EW3C0000711, EW3D0000711, EW3E0000711, EW3F0000711, EW3P0000558, EW3X0000711, EW3Z0000586	Citrix NetScaler 1G SFP Ethernet Long Range (10km) - Single	1310nm (nominal)	9/125um SMF	10 km	SDX 8015/8400/8600, SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, SDX 17500/19500/21500, SDX 22040/22060/22080/22100/22120, SDX 24100/24150

10 GE Pluggable Media

The following table lists the maximum distance specifications for 10G transceivers.

Table 8. Short Reach Fiber 10G SFP+ Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000710, EW3B0000710, EW3C0000710, EW3D0000710, EW3E0000710, EW3F0000710, EW3P0000557, EW3X0000710, EW3Z0000585	Citrix NetScaler 10G SFP+ Ethernet Short Range (300m) - Single	850nm (nominal)	50/125um MMF, 2000MHz-km (OM3)	300 m	SDX 8015/8400/8600, SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, SDX 14020/14030/14040/14060/14080/14100, SDX 17500/19500/21500, SDX 17550/19550/20550/21550, SDX 22040/22060/22080/22100/22120, SDX 24100/24150
			50/125um MMF, 500MHz-km (OM2)	82 m	
			50/125um MMF, 400MHz-km	66 m	
			62.5/125um MMF, 200MHz-km (OM1)	33 m	
			62.5/125um MMF, 160MHz-	26 m	

km

Table 9. Long Reach Fiber 10G SFP+ Distance Specifications

SKU	Description	Transmitter Wavelength (nm)	Fiber Type	Typical Reach (m)	Products
EW3A0000711, EW3B0000711, EW3C0000711, EW3D0000711, EW3E0000711, EW3F0000711, EW3P0000558, EW3X0000711, EW3Z0000586	Citrix NetScaler 10G SFP+ Ethernet Long Range (10km) - Single	1310nm (nominal)	9/125um SMF	10 km	SDX 8015/8400/8600, SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, SDX 14020/14030/14040/14060/14080/14100, SDX 17500/19500/21500, SDX 17550/19550/20550/21550, SDX 22040/22060/22080/22100/22120, SDX 24100/24150

Field Replaceable Units

Jan 28, 2011

Citrix NetScaler field replaceable units (FRU) are NetScaler components that can be quickly and easily removed from the appliance and replaced by the user or a technician at the user's site. The FRUs in a NetScaler appliance can include DC or AC power supplies, and solid-state or hard-disk drives, and a direct attach cable (DAC).

Note: The solid-state or hard-disk drive stores your configuration information, which has to be restored from a backup after replacing the unit.

Power Supply

For appliances containing two power supplies, the second power supply acts as a backup. The SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 appliances can accommodate four power supplies, and require two power supplies for proper operation. The third and fourth power supplies act as backup.

The appliance ships with a standard power cord that plugs into the appliance's power supply and an NEMA 5-15 plug on the other end for connecting to the power outlet on the rack or in the wall.

For power-supply specifications, see "[Hardware Platforms](#)," which describes the various platforms and includes a table summarizing the hardware specifications.

Note: If you suspect that a power-supply fan is not working, please see the description of your platform. On some platforms, what appears to be the fan does not turn, and the actual fan turns only when necessary.

On each power supply, a bicolor LED indicator shows the condition of the power supply.

Electrical Safety Precautions for Power Supply Replacement

- Make sure that the appliance has a direct physical connection to earth ground during normal use. When installing or repairing an appliance, always connect the ground circuit first and disconnect it last.
- Always unplug any appliance before performing repairs or upgrades.
- Never touch a power supply when the power cord is plugged in. As long as the power cord is plugged in, line voltages are present in the power supply even if the power switch is turned off.

Replacing an AC Power Supply

Citrix NetScaler SDX platforms can accommodate two power supplies, except the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 platforms which can accommodate four power supplies. All NetScaler appliances function properly with a single power supply, except the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 platforms which need two power supplies for proper operation. The other power supplies serves as a backup. All power supplies must be of the same type (AC or DC).

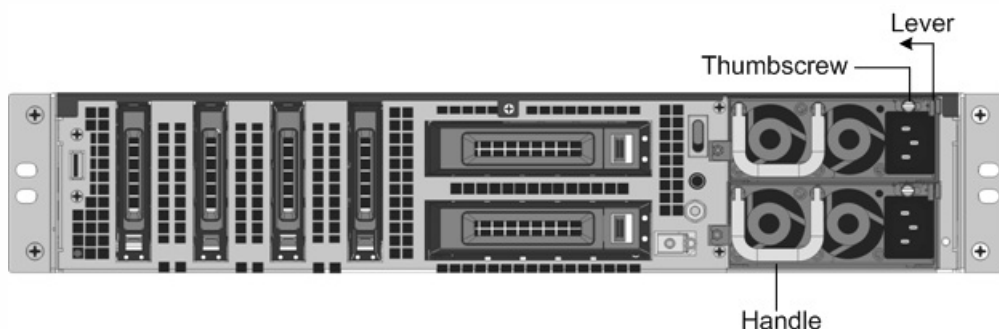
Note: If the appliance has only one power supply, you have to shut down the appliance before replacing the power supply. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace an AC power supply on a Citrix NetScaler appliance

1. Align the semicircular handle perpendicular to the power supply. Loosen the thumbscrew and press the lever toward the handle and pull out the existing power supply, as shown in the following figure.

Note: The illustration in the following figures might not represent the actual NetScaler appliance.

Figure 1. Removing the Existing AC Power Supply



2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.

Figure 2. Inserting the Replacement AC Power Supply



5. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: NetScaler appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

Replacing a DC Power Supply

Citrix NetScaler SDX platforms can accommodate two power supplies, except the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 platforms which can accommodate four power supplies. All NetScaler appliances function properly with a single power supply, except the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 platforms which need two power supplies for proper operation. The other power supplies serves as a backup. All power supplies must be of the same type (AC or DC).

Note: If the appliance has only one power supply, you have to shut down the appliance before replacing the power supply. If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace a DC power supply on a Citrix NetScaler appliance

1. Loosen the thumbscrew and press the lever towards the handle and pull out the existing power supply, as shown in the following figure.

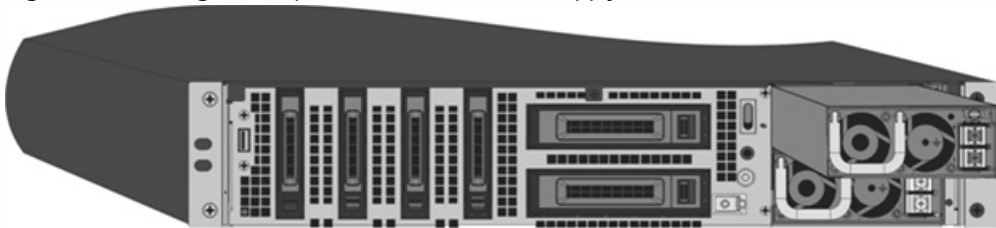
Note: The illustration in the following figures might not represent the actual NetScaler appliance.

Figure 3. Removing the Existing DC Power Supply



2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot while pressing the lever towards the handle. Apply firm pressure to insert the power supply firmly into the slot.

Figure 4. Inserting the Replacement DC Power Supply



5. When the power supply is completely inserted into its slot, release the lever.
6. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: NetScaler appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

Solid-State Drive

A solid-state drive (SSD) is a high-performance device that stores data in solid-state flash memory.

Replacing a Solid-State Drive

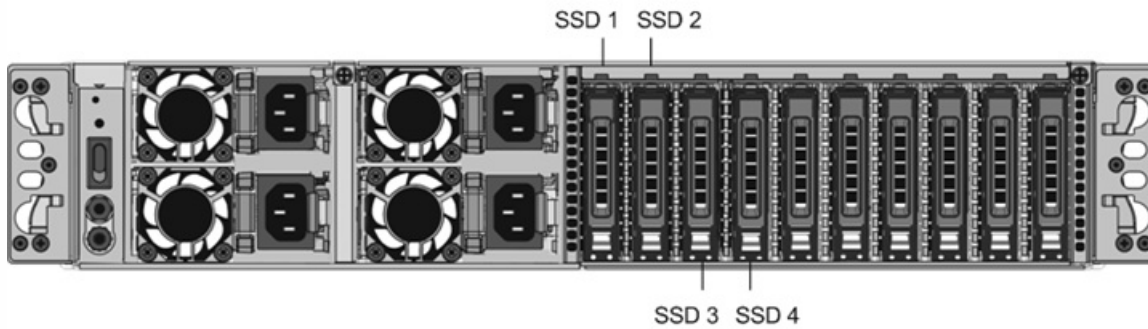
To replace a solid-state drive on SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 appliances

Note: NetScaler SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 appliances are shipped with four SSDs, which contain pre-installed configurations of the NetScaler software. From the left, the first and second SSDs are mirrored and store the configurations of the SDX appliance. The third and fourth SSDs, which are also mirrored, provide storage for the NetScaler instances running on the SDX appliance. All the SSDs are hot-swappable.

You can purchase up to four additional SSDs, in groups of two.

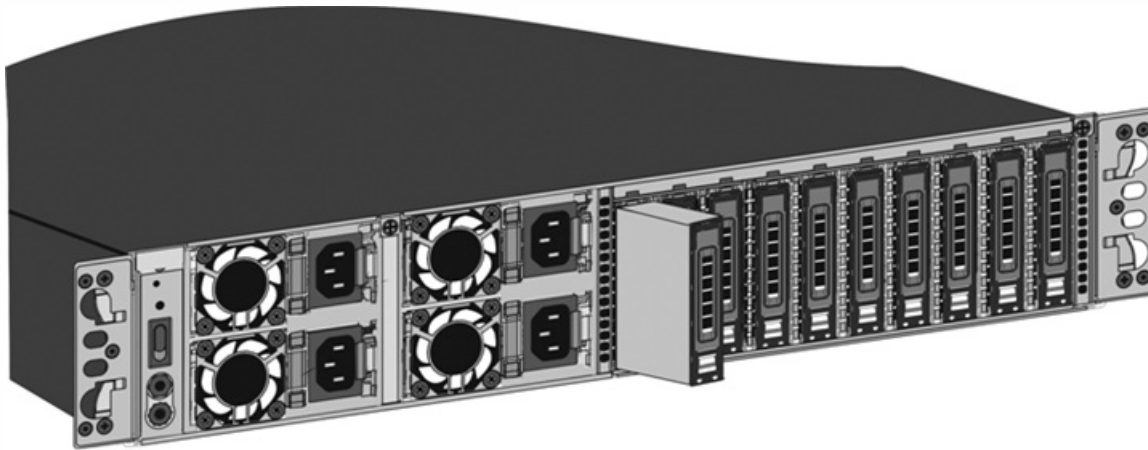
1. Locate the SSD on the back panel of the appliance. Push the safety latch of the drive cover down while pulling out on the drive handle to disengage. Pull out the faulty drive.

Figure 5. Removing the Existing Solid-State Drive



2. Verify that the replacement SSD is of the correct type for the platform.
3. Pick up the new SSD, open the drive handle fully up, and insert the drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the drive locks securely into the slot. Important: When you insert the drive, make sure that the Citrix product label is at the right.

Figure 6. Inserting the Replacement Solid-State Drive



After you replace one of the SSDs, the configuration on the other SSD in the mirrored SSD is copied to the replacement SSD.

Note: NetScaler SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 appliances support up to 80 instances. However, the mirrored SSDs in the third and fourth slots provide only enough storage for up to a maximum of 30 instances. To provision more instances on the appliance, you must purchase and install additional SSDs.

To add additional SSDs on SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 appliances

Put the first new SSD into the leftmost empty slot, and put the second new SSD into the adjacent empty slot.

To replace a solid-state drive on any other SDX appliance

Replacement solid-state drives (SSDs) contain a pre-installed version of the NetScaler software and a generic configuration file (ns.conf), but they do not contain SSL-related certificates and keys, or custom boot settings. After installing the replacement SSD, you have to restore the configuration files and customized settings from backup storage. If no backups are available, you have to reconfigure the appliance. The files to be restored might include:

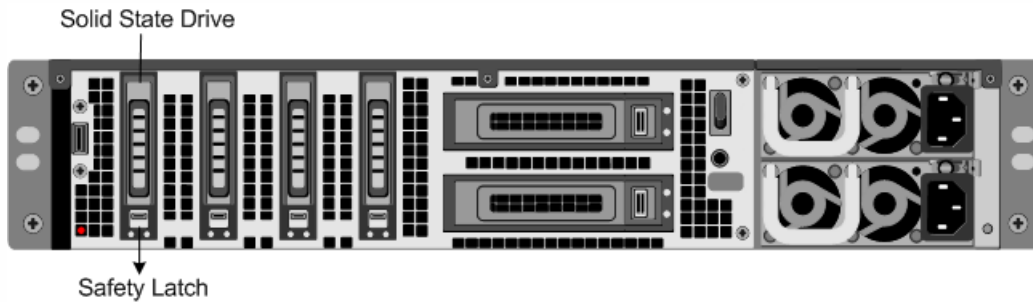
- /flash/nsconfig/ns.conf: The current configuration file.
- /flash/nsconfig/ZebOS.conf: The ZebOS configuration file.
- /flash/nsconfig/license: The licenses for the NetScaler features.
- /flash/nsconfig/ssl: The SSL certificates and keys required for encrypting data sent to clients or servers.

- /nsconfig/rc.netscaler: Customer-specific boot operations (optional).

1. In the configuration utility of the Management Service, navigate to Configuration > System, and in the System pane, click Shut down Appliance.
2. Locate the SSD on the back panel of the appliance. Push the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

Note: The illustration in the following figures might not represent your actual NetScaler appliance.

Figure 7. Removing the Existing Solid-State Drive



3. Verify that the replacement SSD is the correct type for the platform.
4. Pick up the new SSD, open the drive handle fully to the left or up, and insert the drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the drive locks securely into the slot. Important: When you insert the drive, make sure that the Citrix product label is at the top if the drive is inserted horizontally, or at the right if the drive is inserted vertically.

Figure 8. Inserting the Replacement Solid-State Drive



5. Turn on the appliance.
6. Log on to the default IP address by using a web browser, or connect to the serial console by using a console cable, and perform the initial configuration.
7. Upload a platform license and any optional feature licenses, including universal licenses, to the NetScaler appliance.
8. Once the correct NetScaler software version is loaded, you can restore the working configuration. Copy a previous version of the ns.conf file to the /nsconfig directory by using an SCP utility or by pasting the previous configuration into the /nsconfig/ns.conf file from the NetScaler command prompt. To load the new ns.conf file, you must restart the NetScaler appliance by entering the reboot command at the NetScaler command prompt.

Hard Disk Drive

A hard disk drive (HDD) stores logs and other data files. Files stored on the HDD include the newnslog files, dmesg and messages files, and any core/crash files. The HDD comes in various capacities, depending on the Citrix NetScaler platform. Hard drives are used for storing files required at runtime. An HDD is mounted as /var.

Replacing a Hard Disk Drive

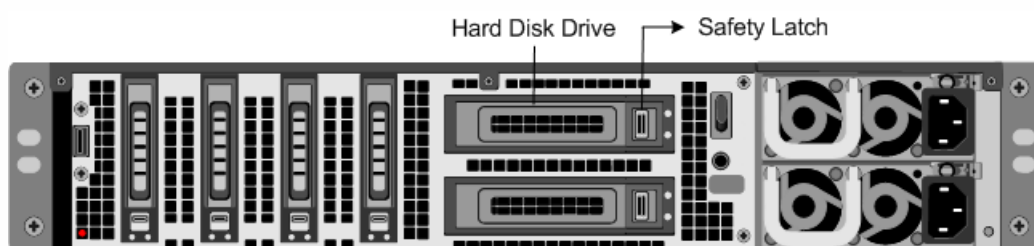
A hard disk drive (HDD) stores log files and other user files. Collection of new log files begins upon boot-up with the new HDD. Product documentation can be downloaded from "[MyCitrix.com](https://mycitrix.com)" and reinstalled to the /var/netScaler/doc location.

To install a hard disk drive

1. Shut down the appliance.
2. Locate the hard disk drive on the back panel of the appliance.
3. Verify that the replacement hard disk drive is the correct type for the NetScaler platform.
4. Disengage the hard disk drive by pushing the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

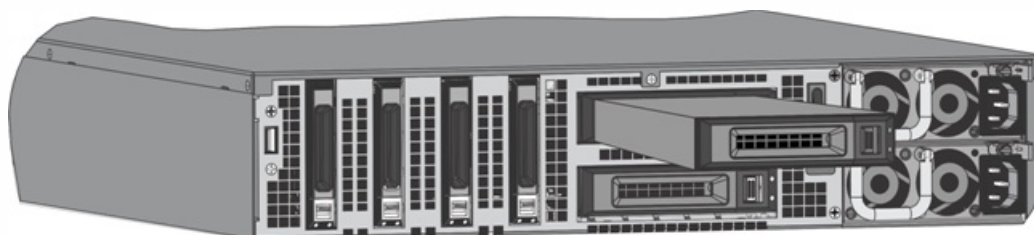
Note: The illustration in the following figures might not represent the actual NetScaler appliance.

Figure 9. Removing the Existing Hard Disk Drive



5. Pick up the new disk drive, open the drive handle fully to the left, and insert the new drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the hard drive locks securely into the slot. Important: When you insert the drive, make sure that the Citrix product label is at the top.

Figure 10. Inserting the Replacement Hard Disk Drive



6. Turn on the NetScaler appliance.

Direct Attach Cable

A direct attach cable (DAC) assembly is a high performance integrated duplex data link for bi-directional communication. The cable is compliant with the IPF MSA (SFF-8432) for mechanical form factor and SFP+ MSA for direct attach cables. The cable, which can be up to 5 meters long, is data-rate agnostic. Supporting speeds in excess of 10 Gbps, it is a cost-effective alternative to optical links (SFP+ transceivers and fiber optic cables.) The transceiver with DAC is hot-swappable. You can insert and remove the transceiver with the attached cable without shutting down the appliance. The Citrix NetScaler appliance supports only passive DAC.

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

Important:

- DAC is supported only on 10G ports. Do not insert a DAC into a 1G port.
- Do not attempt to unplug the integrated copper cable from the transceiver and insert a fiber cable into the transceiver.

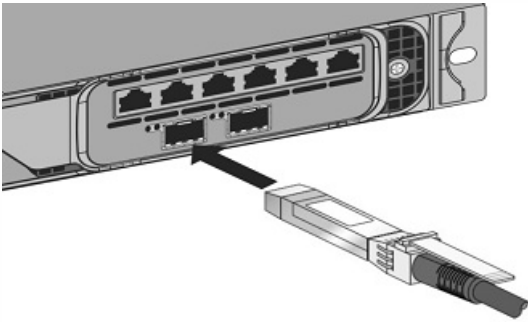
Installing a Direct Attach Cable

Note: The illustrations in the following figures are only for reference and might not represent the actual NetScaler appliance.

To install or remove a direct attach cable

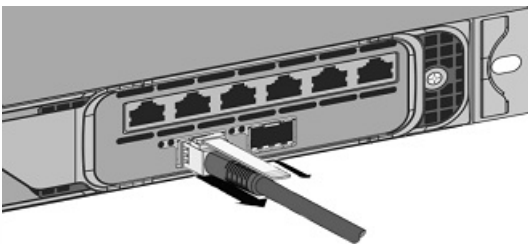
1. To install the DAC, slide it into the 10G port on the appliance, as shown in the following figure. You will hear a click when the DAC properly fits into the port.

Figure 11. Inserting a DAC into the 10G port



2. To remove the DAC, pull the tab on the top of the DAC, and then pull the DAC out of the port, as shown in the following figure.

Figure 12. Removing a DAC from the 10G port



Hardware Platforms

Oct 07, 2013

The various NetScaler hardware platforms offer a wide range of features, communication ports, and processing capacities. All platforms have multicore processors.

The Citrix NetScaler SDX appliance is a multi-tenant platform on which you can provision and manage multiple virtual instances of NetScaler.

The Citrix NetScaler SDX product line consists of:

- Citrix Netscaler SDX 8015/8400/8600
- Citrix Netscaler SDX 11500/13500/14500/16500/18500/20500
- Citrix Netscaler SDX 11515/11520/11530/11540/11542
- Citrix Netscaler SDX 17500/19500/21500
- Citrix Netscaler SDX 17550/19550/20550/21550
- Citrix NetScaler SDX 22040/22060/22080/22100/22120
- Citrix NetScaler SDX 24100/24150

For information on the software releases supported on the NetScaler hardware platforms, see [NetScaler SDX Hardware and Component Compatibility Matrix](#).

Citrix NetScaler SDX 8015, SDX 8400, and SDX 8600

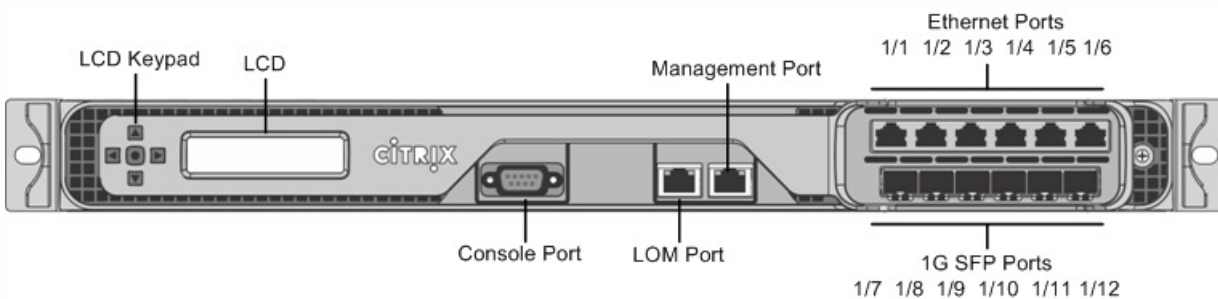
Jan 21, 2014

The Citrix NetScaler models SDX 8015, SDX 8400, and SDX 8600 are 1U appliances. Each model has one quad-core processor (8 cores with hyper-threading) and 32 gigabytes (GB) of memory. The SDX 8015/8400/8600 appliances are available in two port configurations:

- Six 10/100/1000Base-T copper Ethernet ports and six 1G SFP ports (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP)
- Six 10/100/1000Base-T copper Ethernet ports and two 10G SFP+ ports (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+)

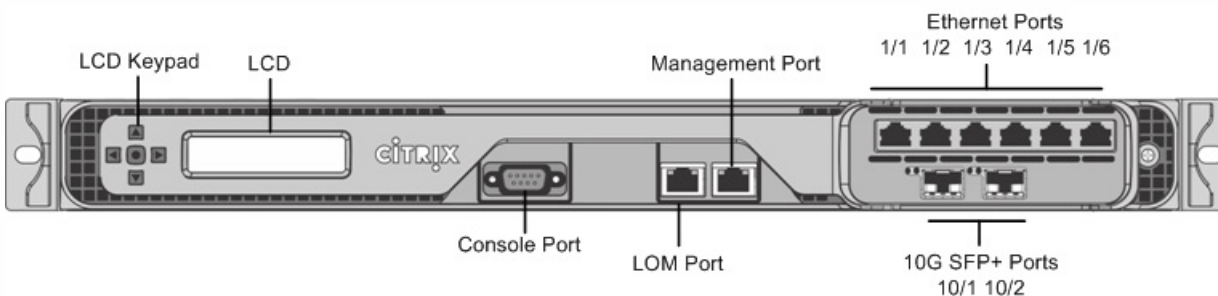
The following figure shows the front panel of the SDX 8015/8400/8600 (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP) appliance.

Figure 1. Citrix NetScaler SDX 8015/8400/8600 (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP), front panel



The following figure shows the front panel of the SDX 8015/8400/8600 (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+) appliance.

Figure 2. Citrix NetScaler SDX 8015/8400/8600 (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+), front panel



Depending on the model, the appliance has the following ports:

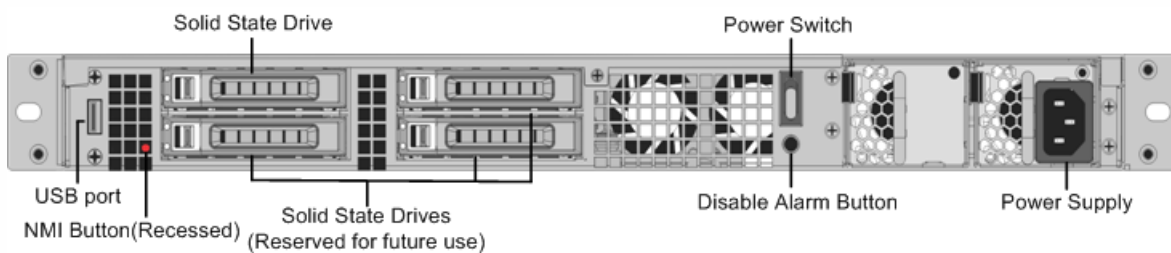
- RS232 serial console port.
- One 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
- One 10/100/1000Base-T copper Ethernet management port (RJ45), numbered 0/1. The management port is used to connect directly to the appliance for system administration functions.
- Network Ports
 - SDX 8015/8400/8600 (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP). Six 10/100/1000BASE-T copper

Ethernet ports (RJ45) numbered 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6 on the top row from left to right, and six 1-gigabit copper or fiber 1G SFP ports numbered 1/7, 1/8, 1/9, 1/10, 1/11, and 1/12 on the bottom row from left to right.

- SDX 8015/8400/8600 (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+). Six 10/100/1000BASE-T copper Ethernet ports (RJ45) numbered 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6 on the top row from left to right and two 10-gigabit SFP+ ports numbered 10/1 and 10/2 on the bottom row from left to right.

The following figure shows the back panel of the SDX 8015/8400/8600 appliance.

Figure 3. Citrix NetScaler SDX 8015/8400/8600 appliance, back panel



The following components are visible on the back panel of the SDX 8015/8400/8600 appliance:

- 256 GB removable solid-state drive, which is used to store the NetScaler software and the user data.
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, which is used at the request of Technical Support to produce a NetScaler core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Disable alarm button, which is nonfunctional. This button is functional only if you install a second power supply. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Single power supply, rated at 450 watts, 110-220 volts.

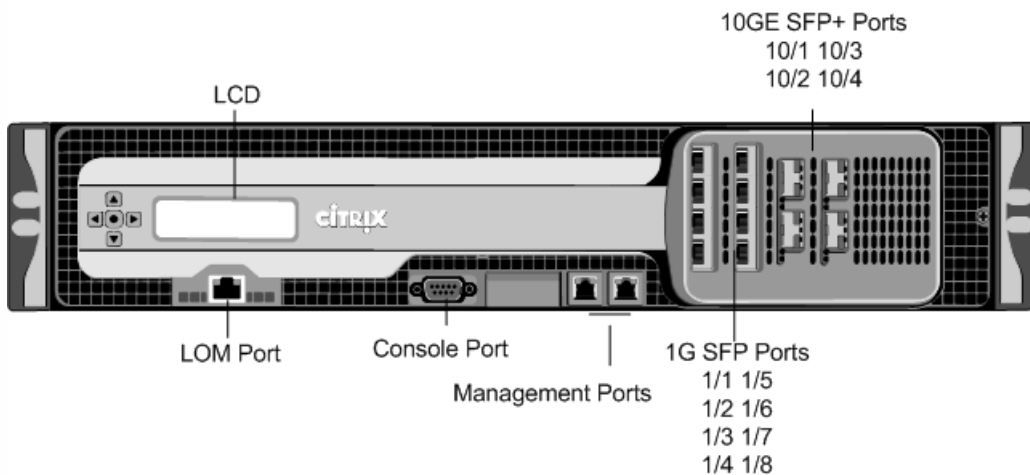
Citrix NetScaler SDX 11500,SDX 13500,SDX 14500,SDX 16500,SDX 18500, andSDX 20500

Oct 25, 2013

The Citrix NetScaler models SDX 11500/13500/14500/16500/18500/20500 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory.

The following figure shows the front panel of the SDX 11500/13500/14500/16500/18500/20500 appliance.

Figure 1. Citrix NetScaler SDX 11500/13500/14500/16500/18500/20500 appliance, front panel

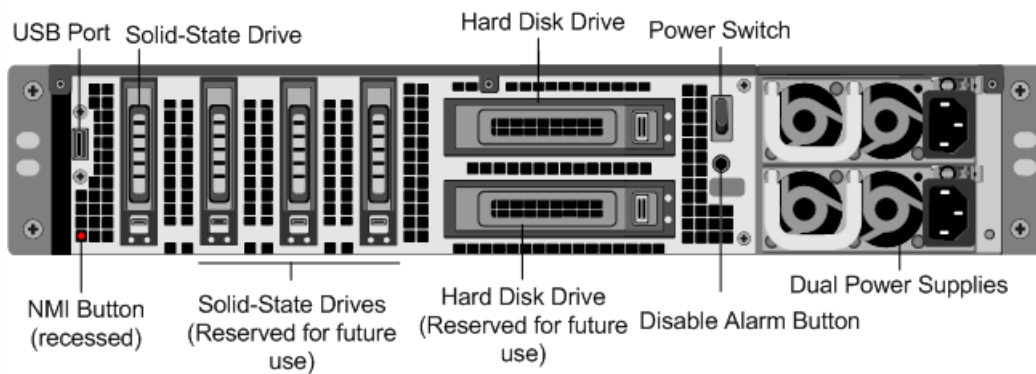


The SDX 11500/13500/14500/16500/18500/20500 appliances have the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
Note: The LEDs on the LOM port are not operational by design.
- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Eight 1G SFP ports numbered 1/1, 1/2, 1/3, 1/4 from top to bottom in the first column, and 1/5, 1/6, 1/7, and 1/8 from top to bottom in the second column.
- Four 10GE SFP+ ports numbered 10/1 and 10/2 from top to bottom in the first column, and 10/3 and 10/4 from top to bottom in the second column.

The following figure shows the back panel of the SDX 11500/13500/14500/16500/18500/20500 appliance.

Figure 2. Citrix NetScaler SDX 11500/13500/14500/16500/18500/20500 appliance, back panel



The following components are visible on the back panel of the SDX 11500/13500/14500/16500/18500/20500 appliance:

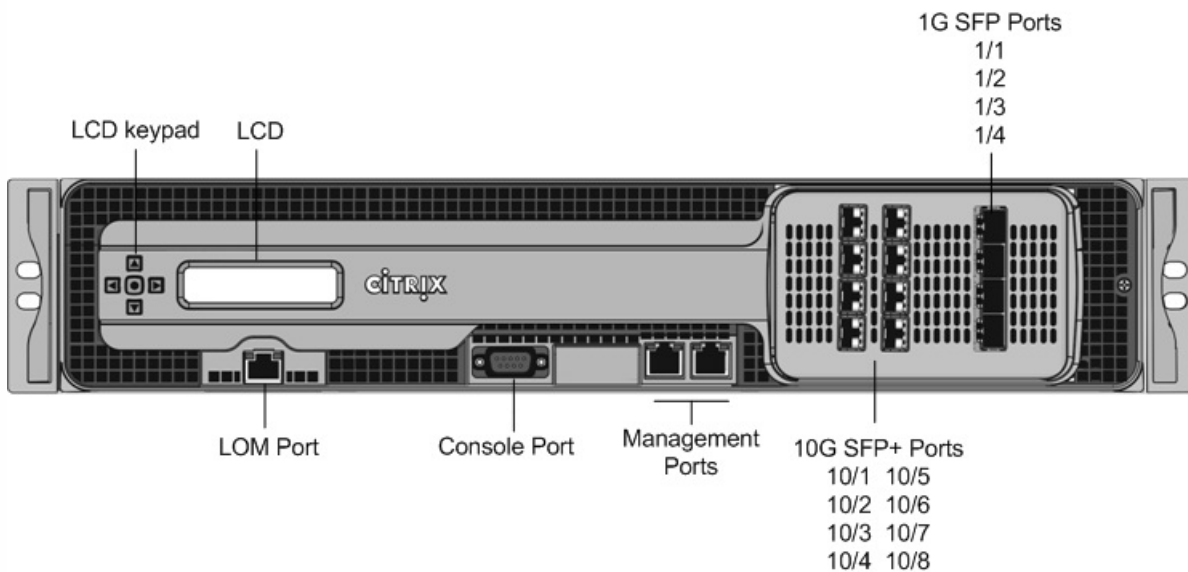
- 160 GB removable solid-state drive that is used to store the NetScaler software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Non-maskable interrupt (NMI) Button that is used at the request of Technical Support and produces a core dump on the NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Two removable hard-disk drives that are used to store user data.
- Disable alarm button. This button is functional only when the appliance has two power supplies. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies, each rated at 650 watts, 110-220 volts.

Citrix NetScaler SDX 11515, SDX 11520, SDX 11530, SDX 11540, and SDX 11542

Mar 14, 2014

The Citrix NetScaler models SDX 11515/11520/11530/11540/11542 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory. The following figure shows the front panel of the SDX 11515/11520/11530/11540/11542 appliance.

Figure 1. Citrix NetScaler SDX 11515/11520/11530/11540/11542 appliance, front panel

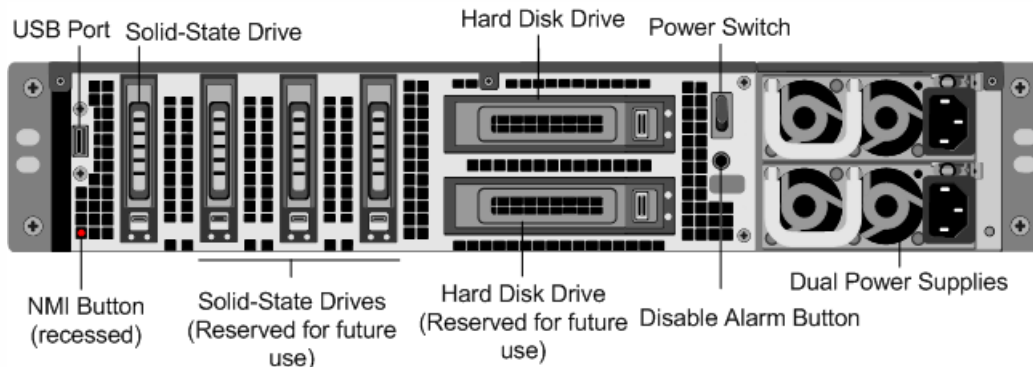


The SDX 11515/11520/11530/11540/11542 appliances have the following ports:

- RS232 serial console port.
- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
Note: The LEDs on the LOM port are not operational by design.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Eight 10G SFP+ ports and four copper or fiber 1G SFP ports.

The following figure shows the back panel of the SDX 11515/11520/11530/11540/11542 appliance.

Figure 3. Citrix NetScaler SDX11515/11520/11530/11540/11542 appliance, back panel



The following components are visible on the back panel of the SDX 11515/11520/11530/11540/11542 appliance:

- 256 GB removable solid-state drive that is used to store the NetScaler software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Non-maskable interrupt (NMI) Button that is used at the request of Technical Support and produces a core dump on the NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Two removable hard-disk drives that are used to store user data.
- Disable alarm button. This button is functional only when the appliance has two power supplies. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies, each rated at 650 watts, 110-220 volts.

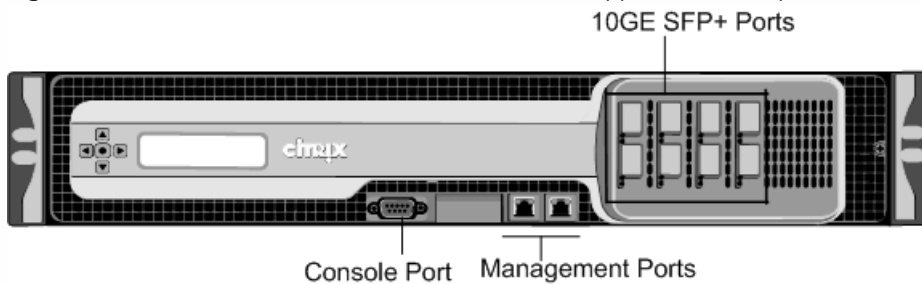
Citrix NetScaler SDX 17500, SDX 19500, and SDX 21500

Oct 25, 2013

The Citrix NetScaler models SDX 17500/19500/21500 are 2U appliances. Each model has two 6-core processors and 48 gigabytes (GB) of memory.

The following figure shows the front panel of the SDX 17500/19500/21500 appliance.

Figure 1. Citrix NetScaler SDX 17500/19500/21500 appliance, front panel

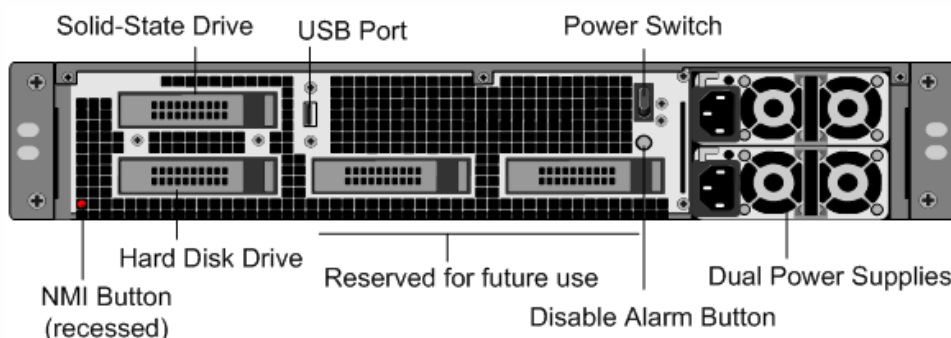


The SDX 17500/19500/21500 appliances have the following ports:

- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Eight 10GE SFP+ ports numbered 10/1, 10/2, 10/3, and 10/4 on the top row from left to right, and 10/5, 10/6, 10/7, and 10/8 on the bottom row from left to right.

The following figure shows the back panel of the SDX 17500/19500/21500 appliance.

Figure 2. Citrix NetScaler SDX 17500/19500/21500 appliance, back panel



The following components are visible on the back panel of the SDX 17500/19500/21500 appliance:

- 160 GB removable solid-state drive that is used to store the NetScaler software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Non-maskable interrupt (NMI) button that is used at the request of Technical Support and produces a core dump on the NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.

- Removable hard-disk drive that stores user data.
- Disable alarm button. This button is functional only when the appliance has two power supplies.
Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies, each rated at 650 watts, 110-220 volts.

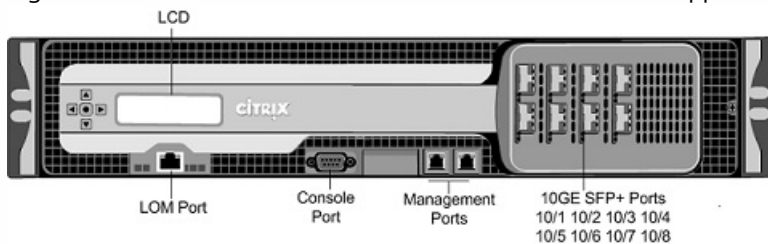
Citrix NetScaler SDX 17550, SDX 19550, SDX 20550, and SDX 21550

Oct 25, 2013

The Citrix NetScaler models SDX 17550, SDX 19550, SDX 20550, and SDX 21550 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 96 gigabytes (GB) of memory.

The following figure shows the front panel of the SDX 17550/19550/20550/21550 appliance.

Figure 1. Citrix NetScaler SDX 17550/19550/20550/21550 appliance, front panel

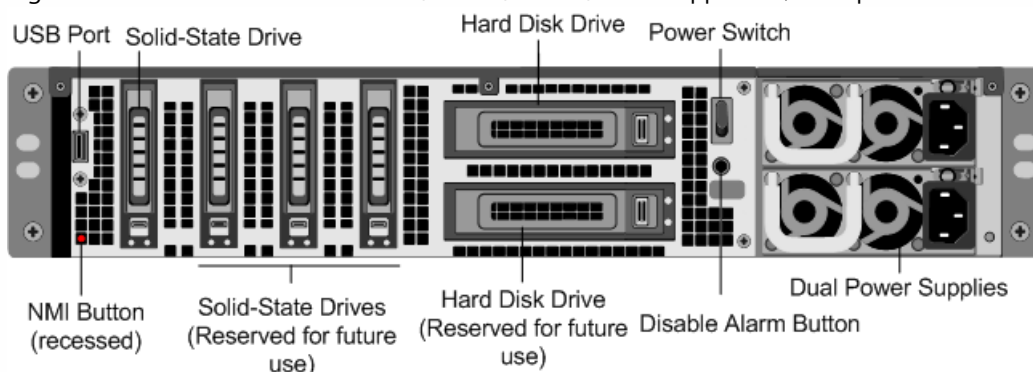


The SDX 17550/19550/20550/21550 appliance has the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
Note: The LEDs on the LOM port are not operational by design.
- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Eight 10GE SFP+ ports numbered 10/1, 10/2, 10/3, and 10/4 on the top row from left to right, and 10/5, 10/6, 10/7, and 10/8 on the bottom row from left to right.

The following figure shows the back panel of the SDX 17550/19550/20550/21550 appliance.

Figure 2. Citrix NetScaler SDX 17550/19550/20550/21550 appliance, back panel



The following components are visible on the back panel of the SDX 17550/19550/20550/21550 appliance:

- 160 GB removable solid-state drive that is used to store the NetScaler software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Non-maskable interrupt (NMI) button that is used at the request of Technical Support and produces a core dump on the

NetScaler. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.

- Two removable hard-disk drives that store user data.
- Disable alarm button. This button is functional only when the appliance has two power supplies. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies, each rated at 850 watts, 110-220 volts.

Citrix NetScaler SDX 22040, SDX 22060, SDX 22080, SDX 22100, and SDX 22120

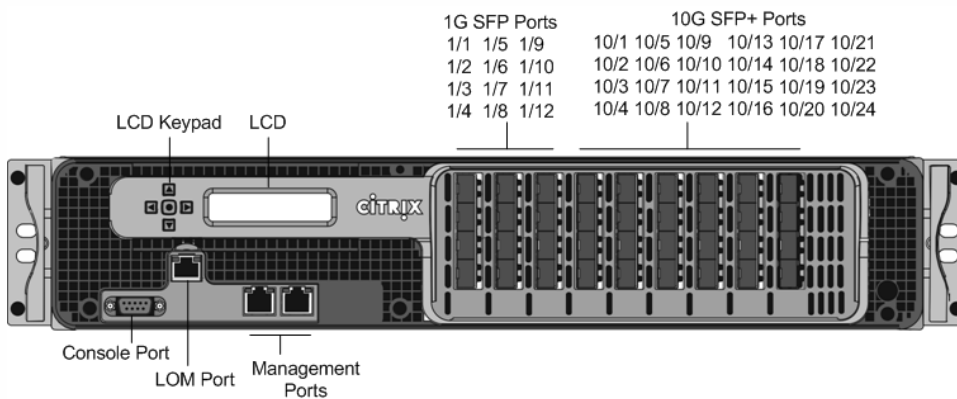
Oct 25, 2013

The Citrix NetScaler SDX 22040/22060/22080/22100/22120 are 2U appliances. Each model has two 8-core processors (32 cores with hyper-threading) and 256 gigabytes (GB) of memory. The SDX 22040/22060/22080/22100/22120 appliances are available in two port configurations:

- Twelve 1G SFP ports and twenty-four 10G SFP+ ports (12x1G SFP + 24x10G SFP+)
- Twenty-four 10G SFP+ ports (24x10G SFP+)

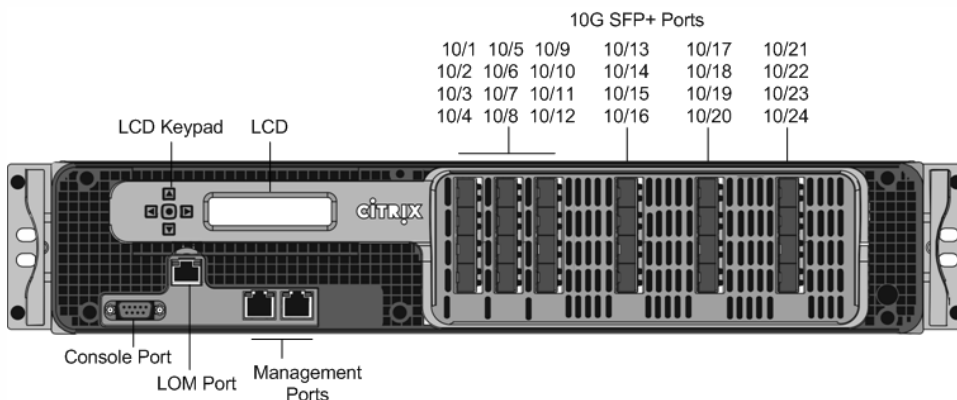
The following figure shows the front panel of the SDX 22040/22060/22080/22100/22120 (12x1G SFP + 24x10G SFP+) appliance.

Figure 1. Citrix NetScaler SDX 22040/22060/22080/22100/22120 (12x1G SFP + 24x10G SFP+), front panel



The following figure shows the front panel of the SDX 22040/22060/22080/22100/22120 (24x10G SFP+) appliance.

Figure 2. Citrix NetScaler SDX 22040/22060/22080/22100/22120 (24x10G SFP+), front panel



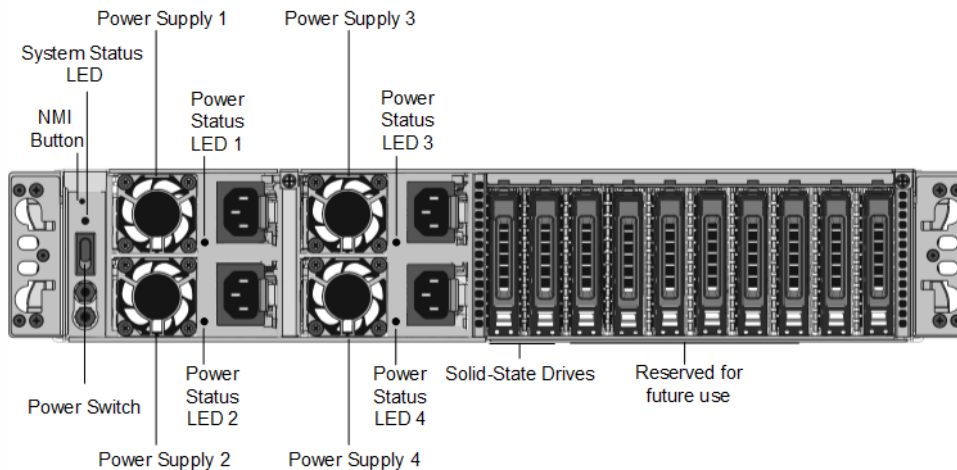
Depending on the model, the appliance has the following ports:

- RS232 serial Console Port.
- 10/100Base-T copper Ethernet Port (RJ45), also called the LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
- Two 10/100/1000Base-T copper Ethernet Management Ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.

- Network Ports
 - SDX 22040/22060/22080/22100/22120 (12x1G SFP + 24x10G SFP+). Twelve copper or fiber 1G SFP ports and twenty-four 10G SFP+ ports.
 - SDX 22040/22060/22080/22100/22120 (24x10G SFP+). Twenty-four 10G SFP+ ports.

The following figure shows the back panel of the SDX 22040/22060/22080/22100/22120 appliances.

Figure 3. Citrix NetScaler SDX 22040/22060/22080/22100/22120, back panel



The following components are visible on the back panel of the SDX 22040/22060/22080/22100/22120 appliance:

- Non-maskable interrupt (NMI) Button, used at the request of Technical Support to initiate a core dump. To press this red button, which is recessed to prevent unintentional activation, use a pen, pencil, or other pointed object. The NMI Button is also available remotely over the network in the LOM GUI, in the Remote Control menu.
- System status LED, which indicates the status of the appliance, as described in <http://support.citrix.com/proddocs/topic/netscaler-hrdwre-installation-10-5/ns-hardware-common-components-ref.html>.

Note: On an SDX 22040/22060/22080/22100/22120 appliance running LOM firmware version 3.22, the system status LED indicates an error (continuously glows RED) even though the appliance is functioning properly.

- Four power supplies, each rated at 750 watts, 100-240 volts. A minimum of two power supplies are required for proper operation. The extra power supplies act as backup. Each power supply has an LED that indicates the status of the power supply, as described in <http://support.citrix.com/proddocs/topic/netscaler-hrdwre-installation-10-5/ns-hardware-common-components-ref.html>.
- Power switch, which turns off power to the appliance. Press the switch for less than two seconds to turn off the power.
- 256 GB removable solid-state drives.

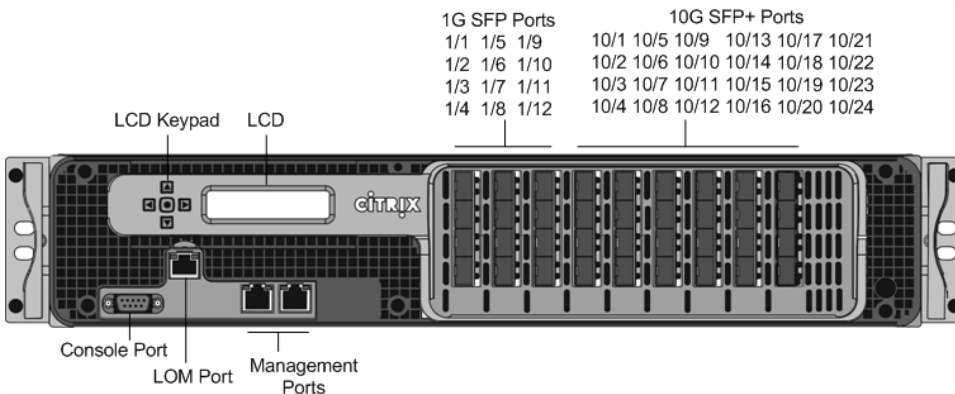
Citrix NetScaler SDX 24100 and SDX 24150

Oct 25, 2013

The Citrix NetScaler SDX 24100/24150 are 2U appliances. Each model has two 8-core processors (32 cores with hyper-threading) and 256 gigabytes (GB) of memory. The SDX 24100/24150 appliances are available in the twelve 1G SFP ports and twenty-four 10G SFP+ ports (12x1G SFP + 24x10G SFP+) configuration.

The following figure shows the front panel of the SDX 24100/24150 (12x1G SFP + 24x10G SFP+) appliance.

Figure 1. Citrix NetScaler SDX 24100/24150 (12x1G SFP + 24x10G SFP+), front panel

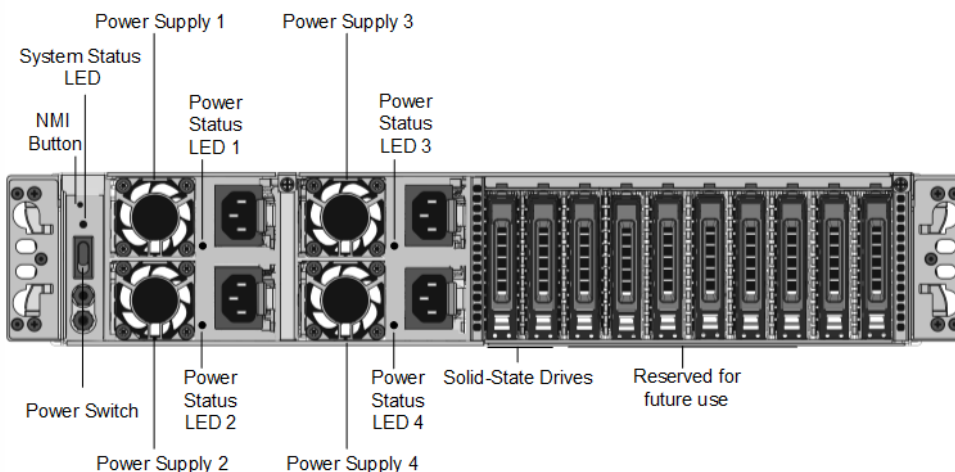


Depending on the model, the appliance has the following ports:

- RS232 serial Console Port.
- 10/100Base-T copper Ethernet Port (RJ45), also called the LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
- Two 10/100/1000Base-T copper Ethernet Management Ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Network Ports
 - SDX 24100/24150 (12x1G SFP + 24x10G SFP+). Twelve copper or fiber 1G SFP ports and twenty-four 10G SFP+ ports.

The following figure shows the back panel of the SDX 24100/24150 appliances.

Figure 2. Citrix NetScaler SDX 24100/24150, back panel



The following components are visible on the back panel of the SDX 24100/24150 appliance:

- Non-maskable interrupt (NMI) Button, used at the request of Technical Support to initiate a core dump. To press this red button, which is recessed to prevent unintentional activation, use a pen, pencil, or other pointed object. The NMI Button is also available remotely over the network in the LOM GUI, in the Remote Control menu.
- System status LED, which indicates the status of the appliance, as described in <http://support.citrix.com/proddocs/topic/netScaler-hrdwre-installation-10-5/ns-hardware-common-components-ref.html>.

Note: On an SDX 24100/24150 appliance running LOM firmware version 3.22, the system status LED indicates an error (continuously glows RED) even though the appliance is functioning properly.

- Four power supplies, each rated at 750 watts, 100-240 volts. A minimum of two power supplies are required for proper operation. The extra power supplies act as backup. Each power supply has an LED that indicates the status of the power supply, as described in <http://support.citrix.com/proddocs/topic/netScaler-hrdwre-installation-10-5/ns-hardware-common-components-ref.html>.
- Power switch, which turns off power to the appliance. Press the switch for less than two seconds to turn off the power.
- Four 600 GB removable solid-state drives. The first two leftmost solid-state drives store the NetScaler software. The next two solid-state drives store user data. Additionally, you can extend the SSD storage (optional) by another 2 or 4 600 GB SSDs.

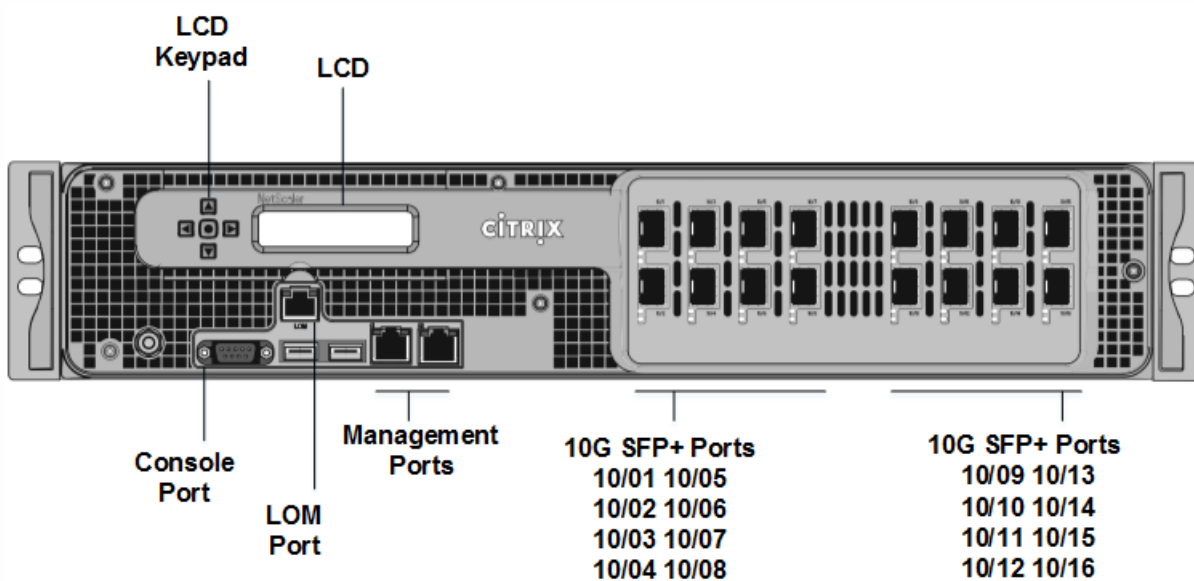
Citrix NetScaler SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 and SDX 14100

Nov 09, 2015

The Citrix NetScaler SDX 14020/14030/14040/14060/14080/14100 are 2U appliances. Each model has two 6-core processors and 64 gigabytes (GB) of memory and sixteen 10G SFP+ ports (16x10G SFP+).

The following figure shows the front panel of the SDX 14020/14030/14040/14060/14080/ 14100 (16x10G SFP+) appliance.

Figure 1. Citrix NetScaler SDX 14020/14030/14040/14060/14080/14100 (16x10G SFP+), front panel



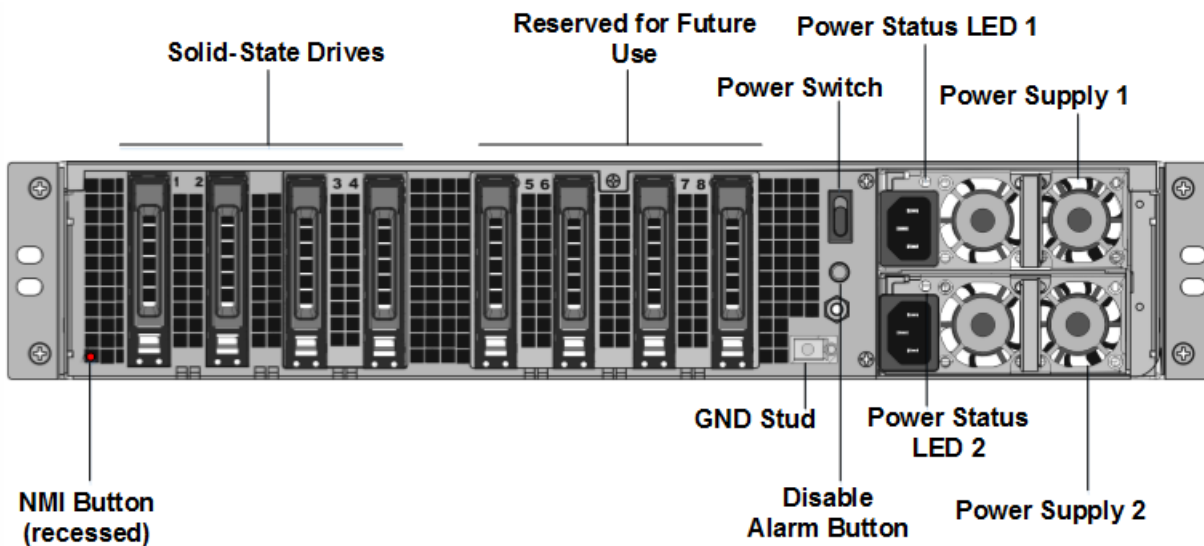
The NetScaler SDX 14020/14030/14040/14060/14080/14100 appliances have the following ports:

- RS232 serial Console Port.
- 10/100Base-T copper Ethernet Port (RJ45), also called the LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
- Two 10/100/1000Base-T copper Ethernet Management Ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions.
- Network Ports, sixteen 10G SFP+ ports (16x10G SFP+).

Note: The 10G SFP+ ports on these appliances support copper 1G SFP transceivers.

The following figure shows the back panel of the SDX 14020/14030/14040/14060/14080/ 14100 appliance.

Figure 2. Citrix NetScaler SDX 14020/14030/14040/14060/14080/14100, back panel



The following components are visible on the back panel of the SDX 14020/14030/14040/14060/14080/14100 appliance:

- Two 240 GB removable solid-state drives (SSDs). The two leftmost solid-state drives store the NetScaler software. The next two solid-state drives, of 300 GB each, store user data. The remaining four solid-state drives are reserved for future use. The NetScaler SDX 14040 appliance has six 300 GB SSDs and NetScaler SDX 14060/14080/14100 appliances have eight 300 GB SSDs. These appliances are redundant array of independent disks (RAID) devices. For more information, see <http://docs.citrix.com/en-us/sdx/11/manage-monitor-appliance-network-configuration/raid-introduction.html>.
- Power switch, which turns power to the appliance on or off. Press the switch for less than two seconds to turn off the power.
- Two power supplies, each rated at 1000 watts, 100-240 volts. Each power supply has an LED that indicates the status of the power supply, as described in <http://docs.citrix.com/en-us/sdx/11/hardware-installation/common-hardware-components.html>.
- Disable alarm button, which is functional only when the appliance has two powersupplies. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet, or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Non-maskable interrupt (NMI) Button, used at the request of Technical Support to initiate a core dump. To press this red button, which is recessed to prevent unintentional activation, use a pen, pencil, or other pointed object. The NMI Button is also available remotely over the network in the LOM GUI, in the Remote Control menu. For more information about the lights out management port of the appliance, see <http://docs.citrix.com/en-us/sdx/11/hardware-installation/lights-out-management-port-lom-of-sdx.html>.

Summary of Hardware Specifications

Apr 01, 2014

The following tables summarize the specifications of the hardware platforms.

Table 1. SDX Platform Summary

	SDX 8015/SDX 8400/SDX 8600	SDX 11500/SDX 13500/SDX 14500/SDX 16500/SDX 18500/SDX 20500	SDX 11515/11520/11530/11540/11542
Processors	1 quad-core (8 cores with hyper-threading)	2 six-core (24 cores with hyper-threading)	2 six-core
Memory	32 GB	48 GB	48 GB
Ports - 1G	<p>6x1G SFP + 6x10/100/1000Base-T copper Ethernet model:</p> <p>6xcopper/fiber 1G SFP ports,</p> <p>6x10/100/1000Base-T copper Ethernet ports</p> <p>2x10G SFP+ 6x10/100/1000Base-T copper Ethernet model:</p> <p>6xcopper/fiber 1G SFP ports,</p>	8x1G SFP ports	<p>8x1G SFP + 4x10G SFP+ model:</p> <p>8xcopper/fiber 1G SFP ports</p> <p>8x1G SFP + 8x10/100/1000Base-T copper Ethernet model:</p> <p>8xcopper/fiber 1G SFP ports,</p> <p>8x10/100/1000Base-T copper Ethernet ports</p>
Ports - 10G	<p>2x10G SFP+ 6x10/100/1000Base-T copper Ethernet model:</p> <p>2x10G SFP+ Ports</p>	4x10G SFP+ ports	<p>8x1G SFP + 4x10G SFP+ model:</p> <p>4x10G SFP+ ports</p>
Number of Power Supplies	1	2	2
Maximum NetScaler Instances	5	20	20

Supported	SDX 8015/SDX 8400/SDX 8600	SDX 11500/SDX 13500/SDX 14500/SDX 16500/SDX 18500/SDX 20500	SDX 11515/11520/11530/11540/11542
AC Power Supply input voltage, frequency, & current	100–240 VAC 50–60 Hz 2.5 A	100–240 VAC 50–60 Hz 6.5–3.5 A	100–240 VAC 50–60 Hz 6.5–3.5 A
Maximum Power Consumption	450 W	650 W	650 W
Heat Dissipation	630 BTU per hour	2200 BTU per hour	2200 BTU per hour
Weight	32 lbs 14.52 kg	46 lbs	46 lbs 20.87 kg
Height	1U	2U	2U
Width	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
Depth	24.01 in or 61 cm	28 in or 71.68 cm	28 in or 71.68 cm
Operating Temperature (degree Celsius)	0–40° C 32–104° F	0–40	0–40° C 32–104° F
Humidity range (non-condensing)	5%–95%	5%-95%	5%–95%
Safety Certifications	TUV	CSA	CSA
EMC & Susceptibility	FCC (Part 15 Class A), CE, C-Tick, VCCI-A	FCC (Part 15 Class A), CE, C-Tick, VCCI, CCC, KC, NOM, GOST, SABS, SASO	FCC (Part 15 Class A), CE, C-Tick, VCCI, CCC, KC, NOM, GOST, SABS, SASO
Compliance	RoHS, WEEE	RoHS, SVHC, WEEE	RoHS, SVHC, WEEE

Table 2. SDX Platform Summary (contd.)

	SDX 17500/SDX 19500/SDX 21500	SDX 17550/SDX 19550/SDX 20550/SDX 21550	SDX 22040/SDX 22060/SDX 22080/SDX 22100/SDX 22120	SDX 24100/SDX 24150
Processors	2 six-core (24 cores with hyper-threading)	2 six-core (24 cores with hyper-threading)	2 eight-core (32 cores with hyper-threading)	2 eight-core (32 cores with hyper-threading)
Memory	48 GB	96 GB	256 GB	256 GB
Ports - 1G	NA	NA	12x1G SFP + 24x10G SFP+ model: 12xcopper/fiber 1G SFP ports	12x1G SFP + 24x10G SFP+ model: 12xcopper/fiber 1G SFP ports
Ports - 10G	8x10G SFP+ ports	8x10G SFP+ ports	12x1G SFP + 24x10G SFP+ model: 24x10G SFP+ ports 24x10G SFP+ ports model: 24x10G SFP+ ports	12x1G SFP + 24x10G SFP+ model: 24x10G SFP+ ports
Number of Power Supplies	2	2	4	4
Maximum NetScaler Instances Supported	20	40	80	80
AC Power Supply input voltage, frequency, & current	100-240 VAC 50-60 Hz 6.5-3.5 A	100-240 VAC 50-60 Hz 6.5-3.5 A	12x1G SFP + 24x10G SFP+ model: 100-240VAC 50/60Hz 6.0-12.0A 24x10G SFP+ model: 100-240VAC	12x1G SFP + 24x10G SFP+ model: 100-240VAC 50/60Hz 6.0-12.0A

	SDX 17500/SDX 19500/SDX 21500	SDX 17550/SDX 19550/SDX 20550/SDX 21550	50/60Hz SDX 22040/SDX 22060/SDX 22080/SDX 6.5-19.5A 22100/SDX 22120	SDX 24100/SDX 24150
Maximum Power Consumption	650 W	850 W	12x1G SFP + 24x10G SFP+ model: 1050 W 24x10G SFP+ model: 1400 W	12x1G SFP + 24x10G SFP+ model: 1050 W
Heat Dissipation	2200 BTU per hour	2900 BTU per hour	12x1G SFP + 24x10G SFP+ model: 2,000-2,6000 BTU per hour 24x10G SFP+ model: 2,700-3,800 BTU per hour	12x1G SFP + 24x10G SFP+ model: 2,000-2,6000 BTU per hour
Weight	40 lbs	40 lbs	85 lbs 38.56 kg	85 lbs 38.56 kg
Height	2U	2U	2U	2U
Width	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
Depth	24.75 in or 62.865 cm	24.75 in or 62.865 cm	28¾ in or 72 cm	28¾ in or 72 cm
Operating Temperature (degree Celsius)	0-40	0-40	0-40° C 32-104° F	0-40° C 32-104° F
Humidity range (non-condensing)	5%-95%	5%-95%	20%-80%	20%-80%
Safety Certifications	TUV	TUV	CSA	CSA
EMC & Susceptibility	FCC (Part 15	FCC (Part 15 Class	FCC (Part 15 Class A), CE	FCC (Part 15 Class A),

Compliance	Class A, CE, C-Tick, VCCI-A SDX 17500/SDX 19500/SDX 21500 RoHS, WEEE	A, CE, C-Tick, VCCI-A SDX 17550/SDX 19550/SDX 20550/SDX 21550 RoHS, WEEE	(EN55022/55024), C-Tick, VCCI SDX 22040/SDX 22060/SDX 22080/SDX 22100/SDX 22120 RoHS, WEEE	CE (EN55022/55024), C-Tick, VCCI SDX 24100/SDX 24150 RoHS, WEEE
------------	---	---	---	--

Table 3. SDX Platform Summary (contd.)

Specifications	SDX 14020/14030/14040/14060/14080/14100
Regulatory model number	Citrix 2U1P1B
Processors	2 six-core
Memory	64 GB
Number of power supplies	2
AC power supply input voltage, frequency, and current	100-240V AC 50-60 Hz 5.9 – 2.95 A
DC power supply input voltage and current	-36V to -72V DC 16.5 – 8.25 A
Maximum AC power consumption	528 W
Maximum DC power consumption	594 W
Airflow (front to rear)	110 CFM Typical 175 CFM Maximum
Heat dissipation	1412 BTU per hour Typical
Package weight (lbs.)	60
System weight (lbs.)	39

Height	2U
Width	EIA 310-D for 19-inch racks
Depth	72 cm; 28¾ in
Operating temperature	0-40°C; 32-104°F
Humidity range (non-condensing)	20%-80%
Safety certifications	CSA
EMC & susceptibility	USA (FCC), Europe (CE), Japan (VCCI), Australia (RCM), China (CCC), Korea (KCC), India (BIS), Mexico (NOM), Saudi Arabia (CITC), South Africa (ICASA), Russia (EAC, CU-TR), Taiwan (BSMI), Brazil (Inmetro & Anatel), Israel (MoE, MoC)
Environmental compliance	WEEE, RoHS, REACH

Preparing for Installation

Jan 28, 2011

Before you install your new appliance, carefully unpack your appliance and make sure that all parts were delivered. Once you are satisfied that your appliance has been delivered to your expectations, verify that the location where the appliance will be installed meets temperature and power requirements and that the server cabinet or floor-to-ceiling cabinet is securely bolted to the floor and has sufficient airflow.

Only trained and qualified personnel should install, maintain, or replace the appliance, and efforts should be taken to ensure that all cautions and warnings are followed.

Unpacking the Appliance

The hardware accessories for your particular appliance, such as cables, adapters, and rail kit, vary depending on the hardware platform you ordered. Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

Use the following list to verify that you received everything that should have been included in the box.

- The appliance you ordered
 - One RJ-45 to DB-9 adapter
 - One 6 ft RJ-45/DB-9 cable
 - The following list specifies the number of power cables included for each appliance model:
 - One power cable for the SDX 8015/8400/8600 appliances
 - Two power cables for the SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, and SDX 17500/19500/21500, and SDX 17550/19550/20550/21550 appliances
 - Four power cables for the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 appliances
- Note: Make sure that a power outlet is available for each cable.

Note: For Brazilian customers, Citrix does not ship a power cable. Use a cable that conforms to the **ABNT NBR 14136:2002** standard.

- One standard 4-post rail kit
- Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process.

- Ethernet cables for each additional Ethernet port that you will connect to your network
 - One available Ethernet port on your network switch or hub for each NetScaler Ethernet port you want to connect to your network
- Note: Transceiver modules are sold separately. Contact your Citrix sales representative to order transceiver modules for your appliance. Only transceivers supplied by Citrix are supported on the appliance.
- A computer to serve as a management workstation

Preparing the Site and Rack

There are specific site and rack requirements for the NetScaler appliance. You must make sure that adequate environmental control and power density are available. Racks must be bolted to the ground, have sufficient airflow, and have adequate power and network connections. Preparing the site and rack are important steps in the installation process and help ensure a smooth installation.

Site Requirements

The appliance should be installed in a server room or server cabinet with the following features:

Environment control

An air conditioner, preferably a dedicated computer room air conditioner (CRAC), capable of maintaining the cabinet or server room at a temperature of no more than 27 degrees C/80.6 degrees F at altitudes of up to 2100 m/7000 ft, or 18 degrees C/64.4 degrees F at higher altitudes, a humidity level no greater than 45 percent, and a dust-free environment.

Power density

Wiring capable of handling at least 4,000 watts per rack unit in addition to power needs for the CRAC.

Rack Requirements

The rack on which you install your appliance should meet the following criteria:

Rack characteristics

Racks should be either integrated into a purpose-designed server cabinet or be the floor-to-ceiling type, bolted down at both top and bottom to ensure stability. If you have a cabinet, it should be installed perpendicular to a load-bearing wall for stability and sufficient airflow. If you have a server room, your racks should be installed in rows spaced at least 1 meter/3 feet apart for sufficient airflow. Your rack must allow your IT personnel unfettered access to the front and back of each server and to all power and network connections.

Power connections

At minimum, two standard power outlets per unit.

Network connections

At minimum, four Ethernet connections per rack unit.

Space requirements

One empty rack unit for the Citrix NetScaler SDX 8015/8400/8600, and two consecutive empty rack units for all other appliance models.

Note: You can order the following rail kits separately.

- Compact 4-post rail kit, which fits racks of 23 to 33 inches.
- 2-post rail kit, which fits 2-post racks.

Cautions and Warnings

Electrical Safety Precautions

Caution: During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.

Follow basic electrical safety precautions to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Remove all jewelry and other metal objects that might come into contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.
- Use a regulating, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and

to keep the appliance operating in case of power failure.

- Never stack the appliance on top of any other server or electronic equipment.
- All appliances are designed to be installed on power systems that use TN earthing. Do not install your device on a power system that uses either TT or IT earthing.
- Make sure that the appliance has a direct physical connection to the earth during normal use. When installing or repairing an appliance, always make sure that the ground circuit is connected first and disconnected last.
- Make sure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 16 A international) is used on all current-carrying conductors on the power system to which your appliances are connected.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, first shut down the appliance, and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload. Always unplug any appliance before performing repairs or upgrades.
- Do not overload the wiring in your server cabinet or on your server room rack.
- During thunderstorms, or anticipated thunderstorms, avoid performing any hardware repairs or upgrades until the danger of lightning has passed.
- When you dispose of an old appliance or any components, follow any local and national laws on disposal of electronic waste.
- To prevent possible explosions, replace expired batteries with the same model or a manufacturer-recommended substitute and follow the manufacturer's instructions for battery replacement.
- Never remove a power supply cover or any sealed part that has the following label:

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no user-serviceable parts inside these components. If you suspect a problem with one of these parts, contact Citrix Technical Support.

Appliance Precautions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment in a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.

- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack. Use the rack-rail hardware, described later, instead.

Installing the Hardware

Jan 31, 2011

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.

Rack Mounting the Appliance

Most appliances can be installed in standard server racks that conform to EIA-310-D specification. The appliances ship with a set of rails, which you must install before you mount the appliance. The only tools that you need for installing an appliance are a Phillips screwdriver and a flathead screwdriver.

Caution: If you are installing the appliance as the only unit in the rack, mount it at the bottom. If the rack contains other units, make sure that the heaviest unit is at the bottom. If the rack has stabilizing devices available, install them before mounting the appliance.

The following table lists the different hardware platforms and the rack units required for each platform.

Table 1. *Height Requirements For Each Platform*

Platform	Number of rack units
SDX 8015/8400/8600	One rack unit
SDX 11500/13500/14500/16500/18500/20500	Two rack units
SDX 11515/11520/11530/11540/11542	Two rack units
SDX 14020/14030/14040/14060/14080/14100	Two rack units
SDX 17500/19500/21500	Two rack units
SDX 17550/19550/20550/21550	Two rack units
SDX 22040/22060/22080/22100/22120	Two rack units
SDX 24100/24150	Two rack units

Each appliance ships with a mounting rail kit that contains two rail assemblies, one for the left side and the other for the right side of the appliance, and screws to attach the rails. An assembly consists of an inner rail and a rack rail. The supplied rail kit is 28 inches long (38 inches extended). Contact your Citrix sales representative to order a 23-inch (33 inches

extended) rail kit.

Note: The same rail kit is used for both square-hole and round-hole racks. See "[Installing the Rail Assembly to the Rack](#)" for specific instructions for threaded, round-hole racks.

To mount the appliance, you must first install the rails and then install the appliance in the rack.

Perform the following tasks to mount the appliance:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

The appliance is shipped with rack-rail hardware. This hardware consists of two inner rails that you attach to the appliance, one on each side, and a rack-rail assembly that you attach to the rack. The following figure illustrates the steps involved in mounting the Citrix NetScaler SDX appliance to a rack.

To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the latch until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the handle on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws: 4 per side for a 1U appliance and 5 per side for a 2U appliance, as shown in the following figure.

Figure 1. Attaching inner rails



4. Repeat steps 1 through 3 to install the left inner rail on the other side of the appliance.

To install the rack rails on the rack

1. If you have a round-hole, threaded rack, skip to step 3.
2. Install square nut retainers into the front post and back post of the rack as shown in the following figures. Before inserting a screw, be sure to align the square nut with the correct hole for your 1U or 2U appliance. The three holes are not evenly spaced.

Figure 2. Installing Retainers into the Front Rack Posts

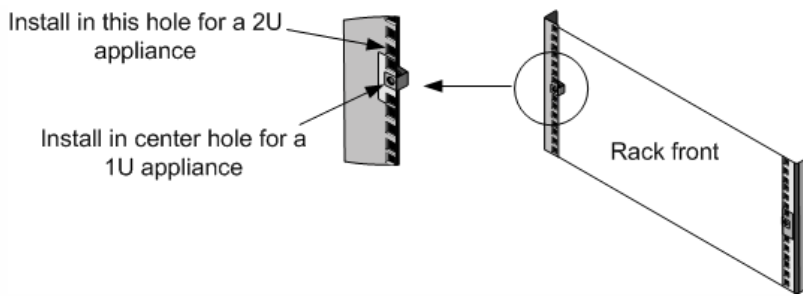
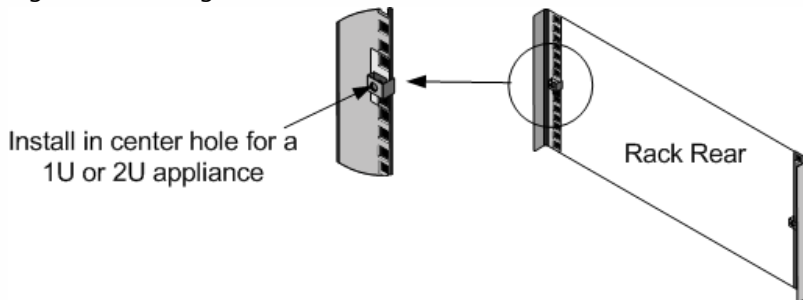
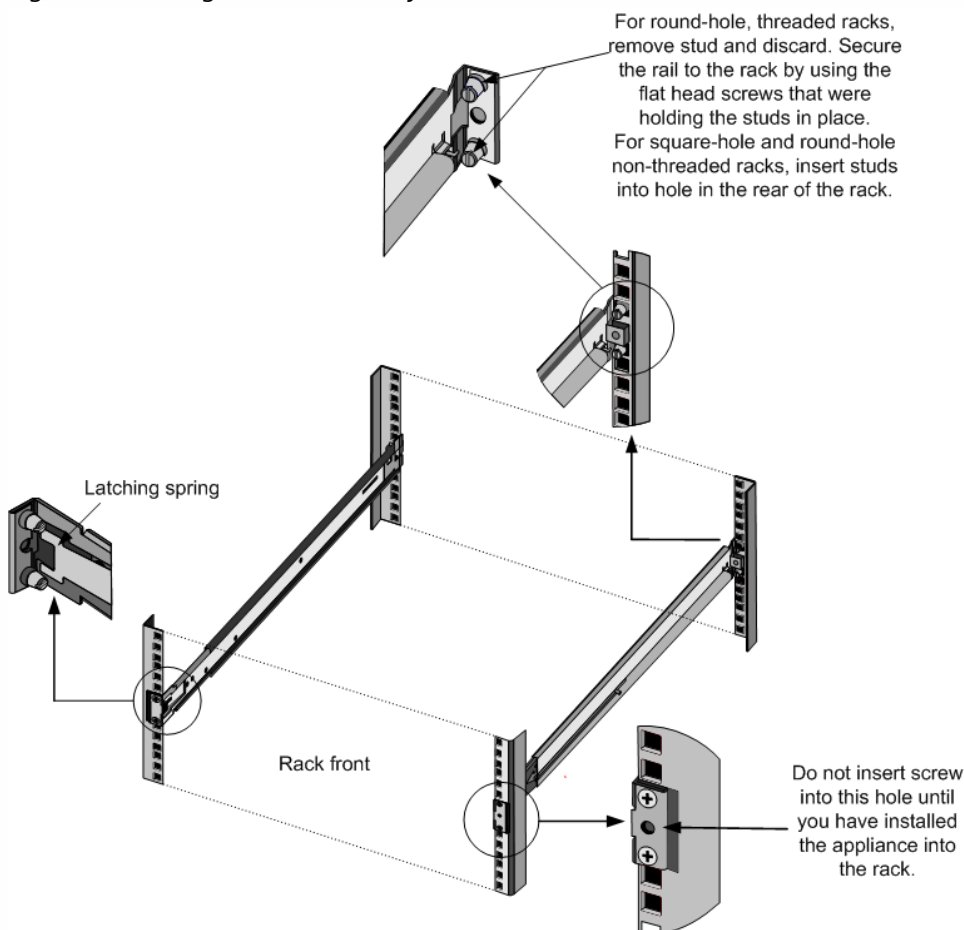


Figure 3. Installing Retainers into the Rear Rack Posts



3. Install the adjustable rail assembly into the rack as shown in the following figures. Use a screw to lock the rear rail flange into the rack. With the screw securing the rail in place, you can optionally remove the latching spring.

Figure 4. Installing the Rail Assembly to the Rack

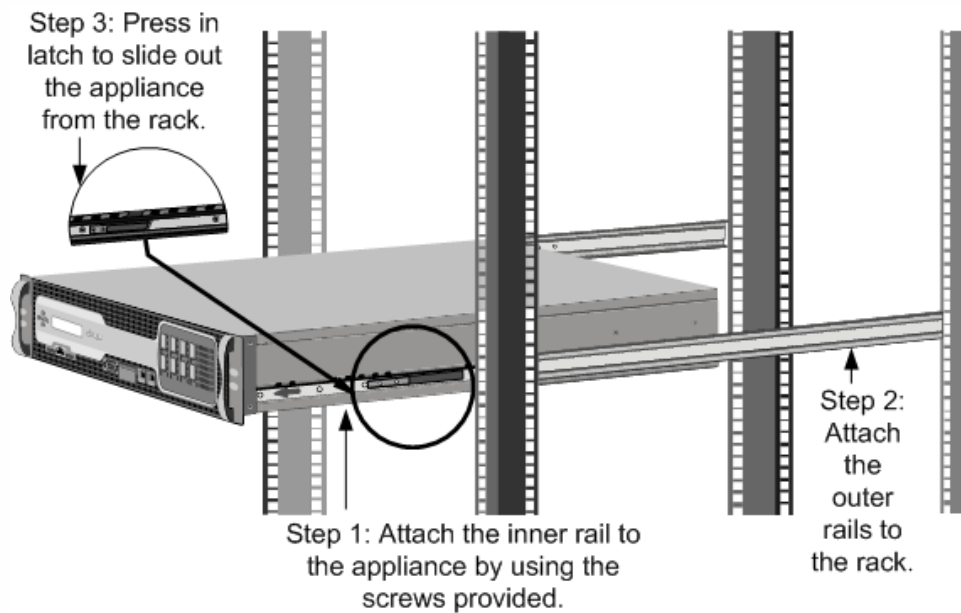


To install the appliance in the rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides.

3. Verify that the appliance is locked in place by pulling it all the way out from the rack.

Figure 5. Rack Mounting the Appliance



Installing and Removing 1G SFP Transceivers

Note: This section applies to the SDX 8015/8400/8600, SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, SDX 22040/22060/22080/22100/22120, and SDX 24100/24150 appliances.

A Small Form-Factor Pluggable (SFP) is a compact transceiver that can operate at speeds of up to 1 gigabit per second and is available in both copper and fiber types. Inserting a 1G SFP copper transceiver converts the 1G SFP port to a 1000BASE-T port. Inserting a 1G SFP fiber transceiver converts the 1G SFP port to a 1000BASE-X port. Auto-negotiation is enabled by default on the 1G SFP port into which you insert your 1G SFP transceiver. As soon as a link between the port and the network is established, the speed and mode are matched on both ends of the cable.

Caution: NetScaler appliances do not support 1G SFP transceivers from vendors other than Citrix Systems. Attempting to install third-party 1G SFP transceivers on your NetScaler appliance voids the warranty.

Insert 1G SFP transceivers into the 1G SFP ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the 1G SFP transceiver or the appliance.

Caution: Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

To install a 1G SFP transceiver

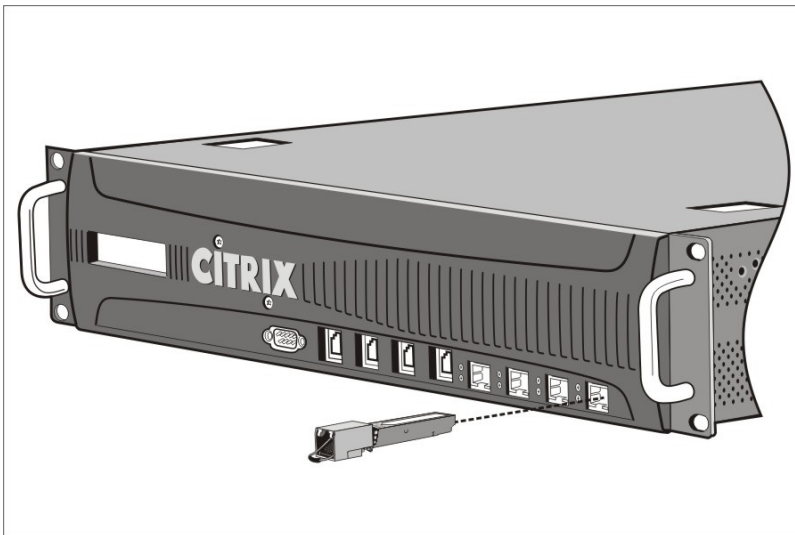
1. Remove the 1G SFP transceiver carefully from its box.

Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Align the 1G SFP transceiver to the front of the 1G SFP transceiver port on the front panel of the appliance, as shown in the following figure.

Note: The illustration in the following figures might not represent your actual appliance.

Figure 6. Installing a 1G SFP transceiver



3. Hold the 1G SFP transceiver between your thumb and index finger and insert it into the 1G SFP transceiver port, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.
5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.
6. If you are using a fiber 1G SFP transceiver, do not remove the dust caps attached to the transceiver and the cable until you are ready to insert the cable.

To remove a 1G SFP transceiver

1. Disconnect the cable from the 1G SFP transceiver. If you are using a fiber optic cable, replace the dust cap on the cable before putting it away.
Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.
2. Unlock the 1G SFP transceiver.
3. Hold the 1G SFP transceiver between your thumb and index finger and slowly pull it out of the port.
4. If you are removing a fiber 1G SFP transceiver, replace the dust cap before putting it away.
5. Put the 1G SFP transceiver into its original box or another appropriate container.

Installing and Removing 10G SFP+ Transceivers

Note: This section applies to the SDX 8015/8400/8600, SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, SDX 14020/14030/14040/14060/14080/14100, SDX 17500/19500/21500, SDX 17550/19550/20550/21550, SDX 22040/22060/22080/22100/22120, and SDX 24100/24150 appliances.

A 10-Gigabit Small Form-Factor Pluggable (SFP+) is a compact optical transceiver that can operate at speeds of up to 10 gigabits per second. Autonegotiation is enabled by default on the 10G SFP+ ports into which you insert your 10G SFP+ transceiver. As soon as a link between the port and the network is established, the mode is matched on both ends of the cable and for 10G SFP+ transceivers, the speed is also autonegotiated.

Caution: NetScaler appliances do not support 10G SFP+ transceivers provided by vendors other than Citrix Systems. Attempting to install third-party 10G SFP+ transceivers on your NetScaler appliance voids the warranty. Insert the 10G SFP+ transceivers into the 10G SFP+ ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the transceiver or the appliance.

Caution: Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

To install a 10G SFP+ transceiver

1. Remove the 10G SFP+ transceiver carefully from its box.
Danger: Do not look directly into fiber optic transceivers and cables. They emit laser beams that can damage your eyes.
2. Align the 10G SFP+ transceiver to the front of the 10G SFP+ transceiver port on the front panel of the appliance.
3. Hold the 10G SFP+ transceiver between your thumb and index finger and insert it into the 10G SFP+ transceiver port, pressing it in until you hear the transceiver snap into place.
4. Move the locking hinge to the DOWN position.
5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.
6. Do not remove the dust caps attached to the transceiver and cable until you are ready to insert the cable.

To remove a 10G SFP+ transceiver

1. Disconnect the cable from the 10G SFP+ transceiver. Replace the dust cap on the cable before putting it away.
Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.
2. Unlock the 10G SFP+ transceiver by moving the locking hinge to the UP position.
3. Hold the 10G SFP+ transceiver between your thumb and index finger and slowly pull it out of the port.
4. Replace the dust cap on the transceiver before putting it away.
5. Put the 10G SFP+ transceiver into its original box or another appropriate container.

Connecting the Cables

When the appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

Danger: Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

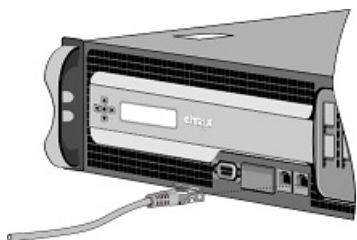
Connecting the Ethernet Cables

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port or 1G SFP copper transceiver. Use a fiber optic cable with an LC duplex connector with a 1G SFP fiber transceiver, 10G SFP+ transceiver. The type of connector at the other end of the fiber optic cable depends on the port of the device that you are connecting to.

To connect an Ethernet cable to a 10/100/1000BASE-T port or 1G SFP copper transceiver

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port on the front panel of the appliance, as shown in the following figure.

Figure 7. Inserting an Ethernet cable



2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.

3. Verify that the LED glows amber when the connection is established.

To connect the Ethernet cable to a 1G SFP fiber, 10G SFP+ transceiver

1. Remove the dust caps from the transceiver and cable.
2. Insert the LC connector on one end of the fiber optic cable into the appropriate port on the front panel of the appliance.
3. Insert the connector on the other end into the target device, such as a router or switch.
4. Verify that the LED glows amber when the connection is established.

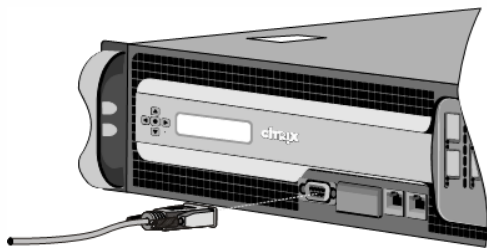
Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Alternatively, you can use a computer connected to the network. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port that is located on the front panel of the appliance, as shown in the following figure.

Figure 8. Inserting a console cable



Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Connecting the Power Cable

An SDX 8015/8400/8600 appliance has one power cable. All the other appliances come with two power cables, but they can also operate if only one power cable is connected. A separate ground cable is not required, because the three-prong plug provides grounding.

To connect the appliance to the power source

1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply, as shown in the following figure.

Figure 9. Inserting a power cable



2. Connect the other end of the power cable to a standard 110V/220V power outlet.
3. If a second power supply is provided, repeat steps 1 and 2 to connect the second power supply.
Note: The SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, SDX 17500/19500/21500, and SDX 17550/19550/20550/21550 appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to the appliance. To silence the alarm, you can press the small red button located on the back panel of the appliance.

Switching on the Appliance

After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. If you have installed a second power supply, make sure the second cable is connected to an outlet for a different circuit than the first. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port. This will ensure that you can configure the appliance after it is switched on.
2. Press the ON/OFF toggle power switch on the back panel of the appliance.

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs you can quickly remove power from the appliance.

Initial Configuration

Apr 09, 2015

After you have installed your appliance in a rack, you are ready to perform the initial configuration. To perform the initial configuration, you can use the Management Service user interface or the serial console. You can access the Management Service user interface from any computer that is on the same network as the new SDX appliance. If you do not have a computer on the same network, use the serial console to perform the initial configuration of the SDX appliance. Citrix recommends that, as soon as you complete the initial configuration, you change the root-user password. For information about changing the root-user password, see .

Determine the following information for performing the initial configuration.

- NetScaler SDX IP address and subnet mask: The management IP address and the mask used to define the subnet in which the SDX appliance is located. This IP address is used to access the NetScaler SDX Management Service user interface.
- XenServer IP address: The IP address of the XenServer hypervisor.
- Default gateway: The IP address of the router that forwards traffic out of the appliance's subnet. The default gateway should be in the same subnet as the NSIP address.
- Root password: The root user (nsroot) has full administrative privileges on the appliance. The root password is used to authenticate the root user. The default root password is nsroot. You can change this password during initial configuration of the appliance.

Initial Configuration through the Management Service User Interface

To set up the appliance by using the Management Service user interface, connect a workstation or laptop to the same network as the appliance.

To configure the NetScaler SDX appliance by using the Management Service user interface

1. Connect the NetScaler SDX appliance to a management workstation or network by using interface 0/1.
2. Open a browser and type: `http://192.168.100.1`
Note: The NetScaler SDX Management Service is preconfigured with the IP address 192.168.100.1 and the XenServer hypervisor is preconfigured with the IP address 192.168.100.2.
3. In the User Name box, type nsroot.
4. In the Password box, type nsroot.
5. In the navigation pane, click System.
6. In the details pane, under Setup Appliance, click Network Configuration and enter values for the following parameters:
 - Interface*—The management interface that connects the appliance to a management workstation or network. 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 that is used to access the Management Service by using a Web browser.
Note: The XenServer IP address and Management Service IP address should be in the same subnet.
 - Netmask*—The mask used to define the subnet in which the SDX appliance is located.
 - Gateway*—The IP address of the router that forwards traffic out of the appliance's subnet.
 - DNS Server—The IP address of the DNS server.

*A required parameter

7. Click OK, and then click Close.
8. To confirm that the NetScaler SDX appliance is configured correctly, you can either ping the new Management Service IP address or use the new IP address to open the user interface in a browser.
Note: After changing the network configuration, close all browser instances and open a new browser instance to access the appliance.

Initial Configuration through the Serial Console

To perform initial configuration of the SDX appliance from outside the L2 domain, connect to the console port of the appliance and follow the instructions carefully.

Note: networkconfig utility is available from build 72.5 and later.

To configure the NetScaler SDX appliance by using the serial console

1. Connect the console cable into your appliance.
2. Connect the other end of the cable to your computer and run the vt100 terminal emulation program of your choice.
 - For Microsoft Windows, you can use HyperTerminal, which is installed with all current versions of Windows.
 - For Apple Macintosh OSX, you can use the GUI-based Terminal program or the shell-based telnet client.
Note: OSX is based on the FreeBSD UNIX platform. Most standard UNIX shell programs are available from the OSX command line.
 - For UNIX-based workstations, you can use the shell-based telnet client or any supported terminal emulation program.
3. Press ENTER. The terminal screen displays the Logon prompt.
Note: You might have to press ENTER two or three times, depending on which terminal program you are using.
4. Log on to the appliance with the administrator credentials. The default credentials for username and password are root and nsroot respectively.
5. At the prompt, type: `ssh nsroot@169.254.0.10` When prompted for the password, type nsroot.
6. At the shell prompt, type: `networkconfig`

You can now use the new IP address to log on to the Management Service user interface.

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.

Lights Out Management Port of the NetScaler SDX Appliance

Dec 17, 2015

The SDX 8005/8015/8200/8400/8600/8800, SDX 11500/13500/14500/16500/18500/20500, SDX 17550/19550/20550/21550, SDX 22040/22060/22080/22100/22120, and SDX 24100/24150 appliances have an Intelligent Platform Management Interface (IPMI), also known as the Lights Out Management (LOM) port, on the front panel of the appliance. You can use the LOM port to remotely monitor and manage the appliance, independently of the NetScaler software.

By connecting the LOM port to a dedicated channel that is separate from the data channel, you can make sure that connectivity to the appliance is maintained even if the data network is down. You thereby eliminate the data cable and data network as a single point of failure.

You can access the LOM port through a browser and use the graphical user interface (GUI) for most tasks. All tasks can be performed through the NetScaler shell.

You can use either the GUI or a shell for the following tasks:

- Configuring the network settings
- Health monitoring
- Power control operations
- Factory reset

Different Citrix appliances support different shells:

- For XenServer based NetScaler SDX and CloudBridge appliances, use the dom0 Linux root shell. To access the dom0 shell, log on to the XenServer management IP address instead of the SDX Management Service IP address, using the “root” account, not the “nsroot” account.
- For Linux based appliances, use the Linux bash root shell.

Note: The terms LOM and Baseboard Management Controller (BMC) are used interchangeably.

Caution: LOM firmware versions are platform specific. Upgrading to a LOM firmware version other than one shown for your platform in the LOM Support Matrix, below, results in the LOM becoming unusable.

The LOM Support Matrix shows the LOM firmware versions shipped with the various platforms, along with the recommended versions, and the earliest NetScaler software versions that support both the shipped and the recommended LOM firmware versions. The latest available LOM package can be found on the Citrix downloads website under [LOM Firmware Upgrade](#).

Hardware	Ships With Version	Recommended Version	Minimum NetScaler Version to avoid PS failure issues
SDX 8005/8015/8200/8400/8600/8800	2.04/2.07/3.02/3.10/3.11	3.11	9.3_65.x, 10.1_123.x, 10.5
SDX 11500/13500/14500/16500/18500/20500	2.52/3.02/3.33/3.39	3.39	9.3_65.x, 10.1_123.x, 10.5

SDX 11515/11520/11530/11540/11542 Hardware	2.52/3.02/3.33/3.39 Ships With Version	3.39 Recommended Version	9.3_65.x, 10.1_123.x, 10.5 Minimum NetScaler Version to avoid PS failure issues
SDX 17550/19550/20550/21550	2.52/3.02/3.33/3.39	3.39	9.3_65.x, 10.1_123.x, 10.5
SDX 22040/22060/22080/22100/22120	2.63/3.22	3.22	9.3_65.x, 10.1_123.x, 10.5
SDX 24100/24150	2.63/3.22	3.22	9.3_65.x, 10.1_123.x, 10.5

Configuring the Network Settings on the LOM Port

Jan 31, 2011

The default IP address for initial access to the LOM port is 192.168.1.3. Change the default credentials and IP address the first time you log on. All LOM GUI operations require you to connect to the appliance by typing the LOM IP address in a web browser and then entering the administrator credentials. Alternatively, you can access LOM functionality through the command line by using the *ipmitool* utility. Using the *ipmitool* utility remotely, you can determine the LOM firmware version number, perform warm and cold restarts, configure LOM network settings, monitor the health of the appliance, and perform power control operations. The utility is available for download at <http://ipmitool.sourceforge.net/>. The *ipmitool* utility is also included in NetScaler MPX and CloudBridge/SDX (dom0) appliances for initial LOM port network configuration. When using the shell, you can choose to use DHCP or static IP settings for initial network configuration. After configuring the network settings, you can use the *ipmitool* commands over the network. For example, the BMC firmware revision command would need the same username, password, and IP address that is used to access the BMC/LOM GUI port.

For initial configuration, connect the network port on your laptop or workstation directly to the LOM port with a crossover cable, or to a switch in the same local subnet(192.168.1.x) as the LOM port. Assign a network-reachable IP address and change the default credentials. After saving the new settings, the LOM restarts and the changes take effect. After the restart, you must use the new address to access to the LOM.

If you make a mistake that results in losing network connectivity at both the old and new IP addresses, you must use the local shell method to recover.

See the [Secure Deployment Guide](#) for best practices for managing administrative credentials and configuring your network for a secure LOM deployment.

Note: On all SDX platforms, except SDX 22040/22060/22080/22100/22120 and SDX 24100/24150, the LEDs on the LOM port are nonoperational by design.

Tip: For first-time setup in a network, to facilitate troubleshooting, make sure that a laptop/PC is connected directly to the LOM port. If you can ping and access the LOM GUI at the default IP address (192.168.1.3) by using static addressing on the laptop/PC, but remote access does not work, take a closer look at network firewall settings and access control list (ACL) policies of all network devices along the network path.

Tip: If some LOM GUI features work but others do not, (for example, normal NetScaler console output is visible in the NetScaler console window in the LOM GUI, but typing in the console does not work), try the above method to isolate the cause to the specific BMC protocol being blocked by the network.

Tip: Some LOM GUI features, such as the NetScaler console, require the latest Java security updates on the laptop/PC. Make sure that the latest Java updates are installed on your laptop/PC.

To configure the NetScaler LOM port by using the GUI

1. In a web browser, type <http://192.168.1.3> and enter the default user credentials.
Note: The NetScaler LOM port is preconfigured with IP address 192.168.1.3 and subnet mask 255.255.255.0.
2. On the Configuration tab, click Network and type new values for the following parameters:
 - IP Address—IP address of the LOM port
 - Subnet Mask—Subnet mask used to define the subnet of the LOM port
 - Default Gateway—IP address of the router that connects the LOM port to the network
3. Click Save.
4. If you want to change the user credentials, navigate to Configuration > Users, select the user, click Modify User, and change the credentials.

To configure the NetScaler LOM port by using the shell

1. Configure the IP addressing mode:

- To use DHCP, at the shell prompt, type:

```
ipmitool lan set 1 ipsrc dhcp
```

No further IP-level configuration is required.

- To use static addressing, at the shell prompt, type:

```
1. ipmitool lan set 1 ipsrc static
```

```
2. ipmitool lan set 1 ipaddr <LOM IP address>
```

```
3. ipmitool lan set 1 netmask <netmask IP address>
```

```
4. ipmitool lan set 1 defgw ipaddr <default gateway IP address>
```

The BMC reboots to apply the changes. Pings to the BMC should succeed after approximately 60 seconds.

2. Optionally, to configure Ethernet VLAN ID and priority, at the NetScaler shell prompt type:

- **ipmitool lan set 1 vlan id <off | <ID>>**

- **ipmitool lan set 1 vlan priority <priority>**

You can either disable or enable the VLAN. Set the VLAN ID to a value from 1 to 4094, and the VLAN priority to a value from 0 to 7. After the network settings have been correctly applied, you can access the ipmitool remotely from a physically separate machine over the network. For remote access, enter the BMC username, BMC password, and the BMC IP address. For example, to run the “ipmitool mc info” command, at the shell prompt on a remote machine, type:

```
ipmitool -U <username> -P <password> -H <bmc IP address> mc info
```

Obtaining Health Monitoring Information

There are two NetScaler MIBs: the NetScaler software management MIB and the NetScaler IPMI LOM hardware management MIB. The software management MIB is primarily used for monitoring the application software and the application software's utilization of hardware resources, such as CPU % and memory %. It provides a high level view of the appliance and is therefore suitable for the application monitoring function carried out by an application group within an organization. The LOM MIB is used for monitoring the hardware health and therefore provides a lower level view of the appliance, more applicable to the network monitoring function carried out by a network monitoring group.

The LOM SNMP traps in the LOM MIB report hardware failures. The NetScaler SNMP traps in the NetScaler MIB report software failures and hardware load issues.

The NetScaler MIB has a very small subset of hardware sensors. It does not cover any BIOS level failures, because the BIOS checks the hardware primarily during boot time, before the NetScaler software starts. If the BIOS detects a failure, it does not load the boot loader. If the boot loader does not load, the operating system does not load, and therefore the NetScaler SNMP software service responsible for sending the traps does not load.

The NetScaler Software Management MIB issues a warning under the following conditions only:

1. If the failure is gradual enough for the main CPU to issue an SNMP alert. An electrical failure close to the CPU, such as a failed electrical capacitor, occurs too quickly for the CPU to issue an alert.
2. If the failure happens after the BIOS, Operating System, and SNMP service have started and normal boot-up has been successful.
3. If the failure happens while the operating system and other system software is in a stable enough state for the SNMP software service to run.

Whenever the NetScaler MIB is unable to report these warnings, because of hardware or software failure, the LOM MIB monitors and reports the warnings. The LOM microcontroller operates independently of the NetScaler software. To monitor the hardware and software of the NetScaler appliance, you must use both the NetScaler MIB and the LOM MIB.

The NetScaler IPMI LOM hardware management MIB SNMP firmware runs on the BMC microcontroller chip. The BMC chip CPU sends a warning in the case of a hardware failure, regardless of whether any of the above conditions occurs. For example, if the BIOS halts the system during boot-up because of a memory DIMM failure, the BMC chip uses the BIOS POST code snooping mechanism to detect the failure, and sends a bad DIMM SNMP alert.

You can log on to the LOM port to view the health information about the appliance. All system sensor information, such as system temperature, CPU temperature, and status of fans and power supplies, appears on the sensor readings page. The Event Log records time stamps of routine events such as a power cycle, in addition to recording hardware-failure events. If SNMP traps are enabled, these events can be sent to your SNMP Network Monitoring software. For more information about how to set up an SNMP alert, see [Configuring SNMP Alerts](#).

To obtain health monitoring information

1. In the Menu bar, click System Health.
2. Under Options, click Sensor Readings.

Installing the MIB

Download the IPMI SNMP management information base (MIB) for your LOM firmware version, and import it into the SNMP monitoring software.

For a sample configuration, see <http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap.html>. For the exact steps of this procedure specific to your environment, contact your SNMP network monitoring software provider.

Configuring SNMP Alerts

You can configure SNMP alerts on the LOM. Optionally, you can configure an alert to send emails.

To configure the alerts, you can use the LOM GUI or the NetScaler Shell.

To configure SNMP alerts on the LOM by using the GUI

1. Download the IPMI View utility from <ftp://ftp.supermicro.com/utility/IPMIView/> and install it on your computer. You will use this utility to test the configuration. For more information, see the section about configuring the alert settings in the IPMI View User Guide at <http://supermicro.com>.
2. Open the IPMI View utility.
3. In the LOM GUI, navigate to Configuration > Alerts, click Alert No 1, and then click Modify.
4. Select the severity level of the events for which to generate alerts.
5. Set Destination IP to the IP address at which you installed the IPMI View utility.
6. Optionally, to receive alerts by email, specify an email address. To avoid receiving email for routine alerts, specify a severity higher than Informational.
7. Click Save.
8. The LOM should start sending alerts to the IPMI View utility within a minute or two. After the IPMI View utility starts receiving alerts from the LOM, reconfigure the destination IP address to point to your SNMP Network Management Software, such as HP OpenView.

Setting up SNMP Alerts on the LOM by Using the NetScaler Shell

To customize your filter and policy settings, see the IPMI Specification 2.0 rev. 1.1 documentation.

The latest IPMI specifications are available from the IPMI section of the Intel website:

<http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-specifications.html>

Usually, customization in the SNMP Network Management Software is the preferred method, because it can be done one time at a central location. Therefore, the settings below send all events for all sensors to the SNMP network management software. These are very low traffic events and therefore should not result in any significant network usage.

To set up SNMP filters

The following commands set up SNMP to allow all events:

```
ipmitool raw 4 0x12 0x6 0x10 0x80 1 1 0 0xff 0xff 0xff 0xff 0xff 0xff 0 0xff 0 0 0xff 0 0 0xff 0
```

To set up a policy list

The following command creates a policy list for all sensors and events:

```
ipmitool raw 4 0x12 9 0x10 0x18 0x11 0x81
```

To setting up the destination address for SNMP events

The following command sets up a destination IP address for an SNMP event:

```
ipmitool lan alert set 1 1 ipaddr <x.x.x.x>
```

Where, <x.x.x.x> is the IP address to which the SNMP event should be sent.

To specify an SNMP community string name

At the prompt, type:

```
ipmitool lan set 1 snmp <community string>
```

Installing a Certificate and Key on the LOM GUI

Jan 31, 2011

Citrix recommends using HTTPS to access the LOM GUI. To use HTTPS, you must replace the default SSL certificate with one from a trusted certificate authority and upload a private key to the LOM GUI.

To encrypt SNMP alerts, setup an SSL certificate and private key. In the GUI, navigate to **Configuration > SSL Certification** and apply the SSL certificate and private key. See the NetScaler Secure Deployment Guide for more information about how to securely deploy the LOM in your network. To enable encryption and learn the security measures for LOM, see <http://support.citrix.com/article/CTX129514>.

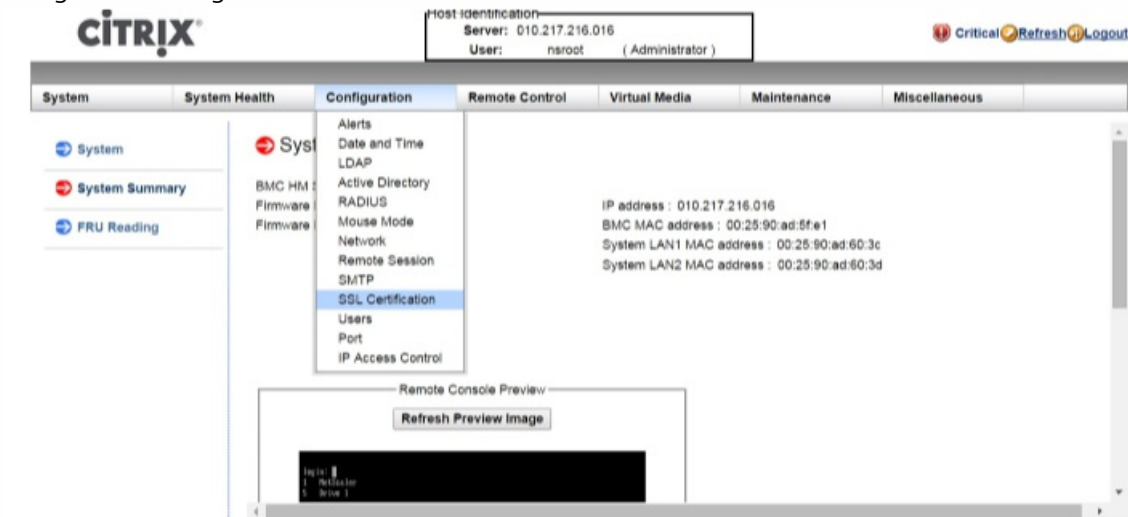
If you make a mistake, you must restore the BMC to the factory defaults to erase the certificate and key. Use the following shell command:

```
ipmitool raw 0x30 0x41 0x1
```

Note: The certificate file must contain only the certificate. The certificate and key must not be in the same file. Make sure that the certificate contains only the certificate and that the key file contains only the key.

To upload a trusted certificate and private key by using the LOM GUI

1. Navigate to Configuration > SSL Certification.



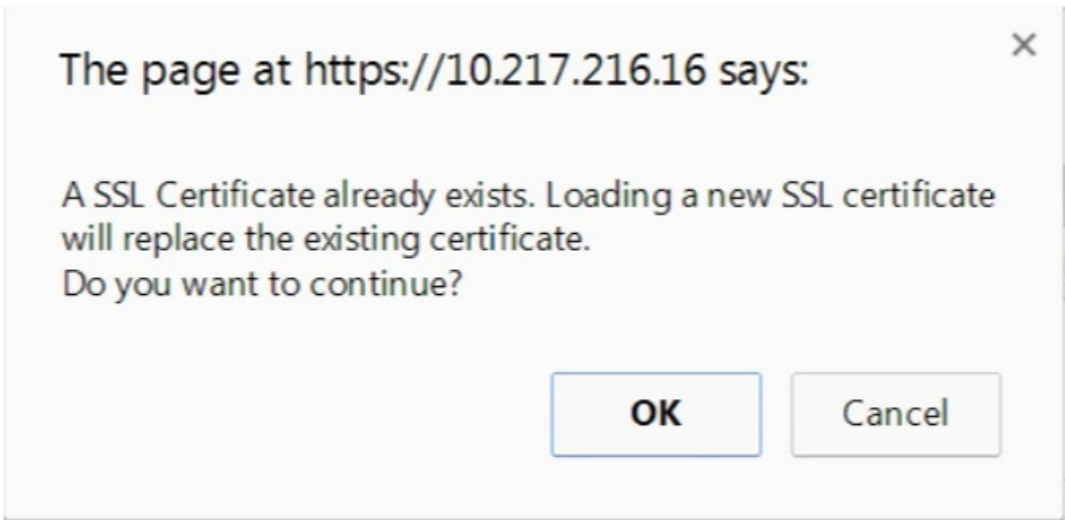
2. In the right pane, click the Choose File buttons to select a new SSL certificate and a new private key.

The screenshot shows the Citrix management console interface. At the top, the Citrix logo is on the left, and the host identification box shows 'Server: 010.217.216.016' and 'User: nsroot (Administrator)'. On the right, there are 'Critical', 'Refresh', and 'Logout' buttons. Below this is a navigation bar with tabs: System, System Health, Configuration, Remote Control, Virtual Media, Maintenance, and Miscellaneous. A left sidebar contains a list of configuration options: Configuration, Alerts, Date and Time, LDAP, Active Directory, RADIUS, Mouse Mode, Network, Remote Session, SMTP, and SSL Certification (which is highlighted with a red arrow). The main content area is titled 'SSL Upload' and contains a message: 'The validity of the default certificate is shown below. To renew SSL certificate, please upload New SSL Certificate and New Private Key.' Below this message, there are two rows of information: 'Certification Valid From' (2/8/2011 10:36:37 PM) and 'Certification Valid Until' (1/31/2041 10:36:37 PM). Underneath, there are two rows for file selection: 'New SSL Certificate' and 'New Private Key'. Each row has a 'Choose File' button followed by the text 'No file chosen'. At the bottom of the form is an 'Upload' button.

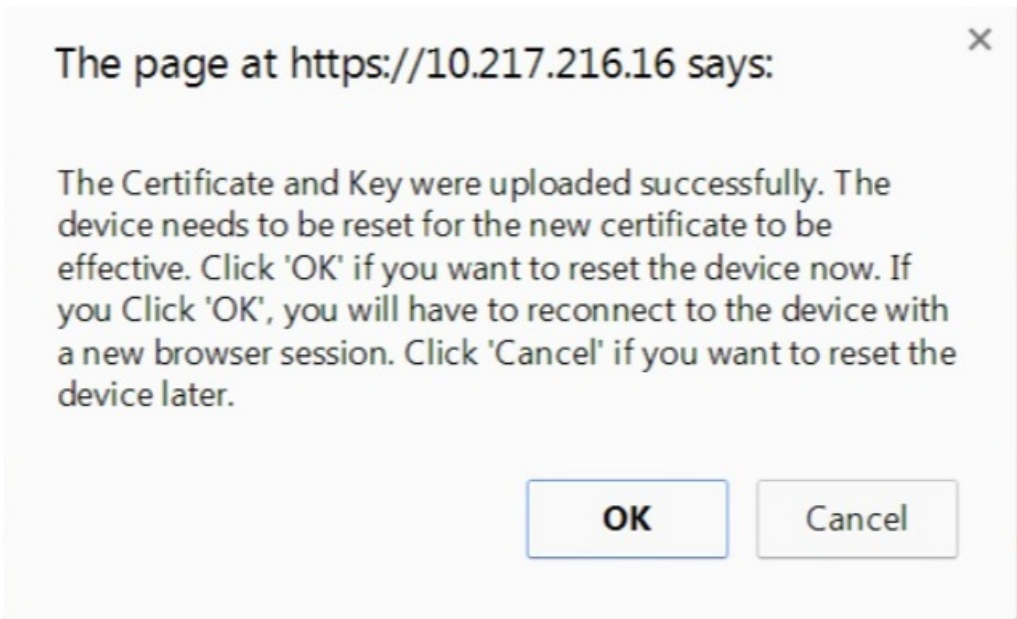
- To verify that you have selected the correct certificate and private key, check the file names of the certificate and key, which appear next to the Choose File buttons.

This screenshot is identical to the one above, but the file selection fields are now populated. The 'New SSL Certificate' row shows the 'Choose File' button followed by the filename 'certbundle-one.pem'. The 'New Private Key' row shows the 'Choose File' button followed by the filename 'certkey.pem'. The 'Upload' button remains at the bottom of the form.

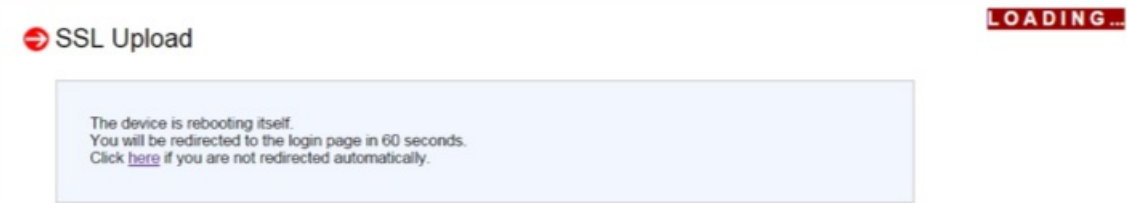
- Click Upload. A message informs you that uploading a new SSL certificate replaces the existing (default) certificate.
- Click OK.



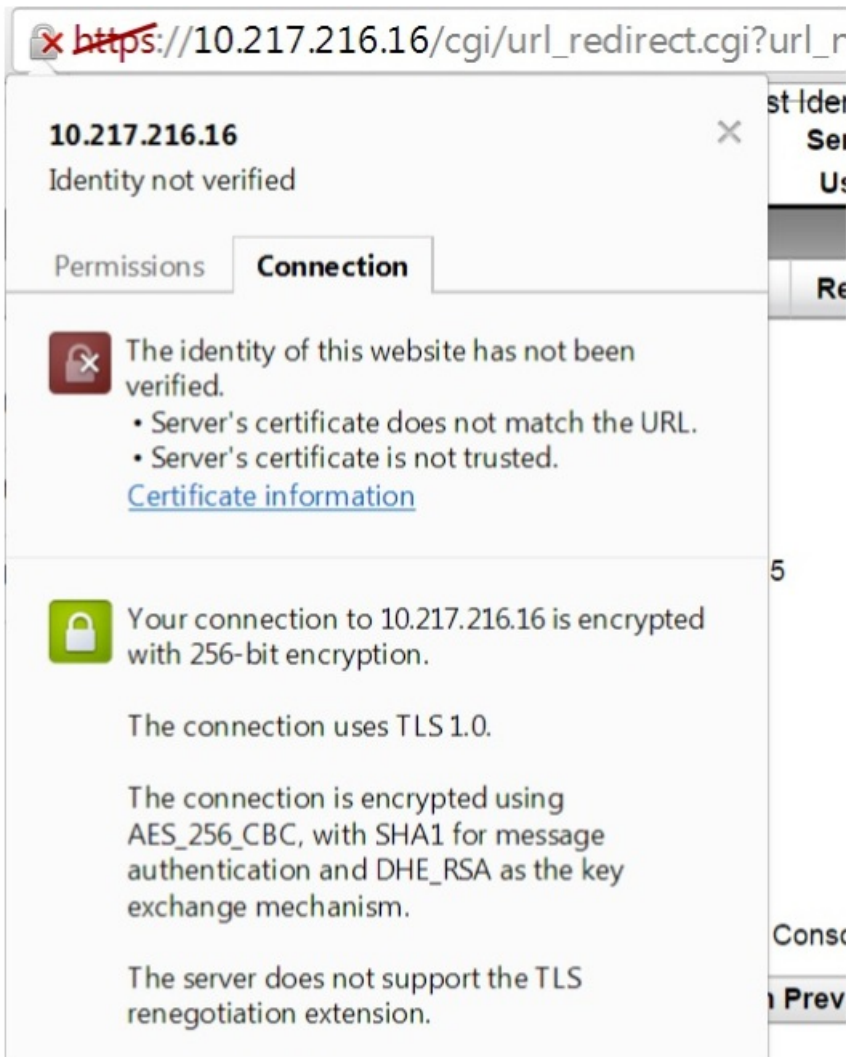
6. When a message informs you that the certificate and key have been uploaded successfully, click OK to reset the device.



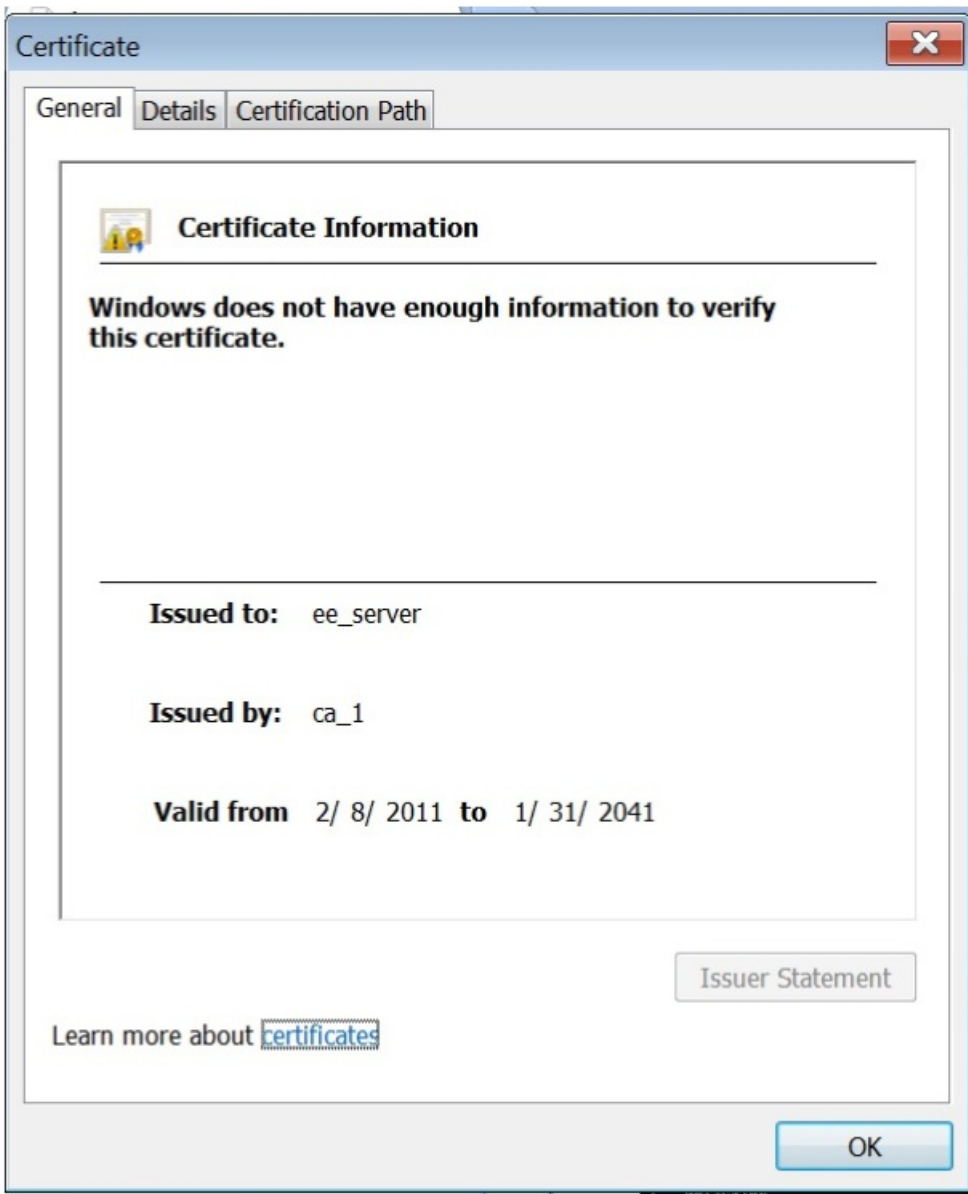
The reset takes approximately 60 seconds. You are then redirected to the logon page.



7. Log on to the LOM GUI by using your default credentials.
Note: If the certificate or key are invalid, the BMC reboots, tries the new settings, and reverts to using the previous settings.
8. In the address bar, click the lock icon to display the connection tab, as shown on the screen below.



9. Click Certificate information to display details about the certificate that you just uploaded.



Note: For the best practices for LOM and NetScaler security, see <http://support.citrix.com/article/CTX129514>.

Obtaining the MAC Address, Serial Number, and Host Properties of the Appliance

Jan 31, 2011

A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communication on the physical network segment. The serial number is on the back panel of the appliance. If you do not have easy access to the back panel, you can get the appliance's serial number by logging on to the LOM port. You can also retrieve the parameter settings assigned to the IP addresses configured on the appliance, such as the state of ARP, ICMP, telnet, secure shell access, and dynamic routing.

To obtain the MAC address, serial number, and host properties of the appliance by using the LOM GUI

1. In the Menu bar, click Remote Control.
2. Under Options, click Console Redirection.
3. Click Launch Console, and then click Yes.
4. Type the administrator credentials.
5. Type `show interface <management_interface_id>` to display the MAC address.
6. Type `show hardware` to display the serial number of the appliance.
7. Type `sh nsip` to display the host properties of the appliance.

To obtain the MAC address and host properties of the BMC by using the appliance shell

At the shell prompt, type:

```
ipmitool lan print
```

Example

```
Set in Progress      : Set Complete
Auth Type Support    : MD2 MD5 OEM
Auth Type Enable     : Callback : MD2 MD5 OEM
                    : User      : MD2 MD5 OEM
                    : Operator  : MD2 MD5 OEM
                    : Admin    : MD2 MD5 OEM
                    : OEM      :
IP Address Source    : Static Address
IP Address           : 192.168.1.3
Subnet Mask          : 255.255.255.0
MAC Address          : 00:25:90:3f:5e:d0
SNMP Community String : public
IP Header            : TTL=0x00 Flags=0x00 Precedence=0x00 TOS=0x00
BMC ARP Control      : ARP Responses Enabled, Gratuitous ARP Disabled
Gratuitous ARP Intrvl : 0.0 seconds
Default Gateway IP   : 0.0.0.0
Default Gateway MAC  : 00:00:00:00:00:00
Backup Gateway IP    : 0.0.0.0
Backup Gateway MAC   : 00:00:00:00:00:00
```

802.1q VLAN ID : Disabled
802.1q VLAN Priority : 0
RMCP+ Cipher Suites : 1,2,3,6,7,8,11,12,0
Cipher Suite Priv Max : aaaaXXaaaXXaaXX
: X=Cipher Suite Unused
: c=CALLBACK
: u=USER
: o=OPERATOR
: a=ADMIN
: O=OEM

Performing Power Control Operations by using the LOM Port

Jan 31, 2011

Through the LOM port, you can remotely perform power control operations, such as graceful shutdown and restart, power cycling the appliance, and restarting the BMC microcontroller. A cold restart takes longer than a warm restart. In a cold restart, you switch off power to the appliance and then switch it back on.

To perform power control operations by using the GUI

1. In the Menu bar, click Remote Control.
2. Under Options, click Power Control, and then select one of the following options:
 - **Reset System**— Gracefully restart the appliance. All operations on the appliance are stopped, no new connections to the client or server are accepted, and all existing connections are closed before the appliance restarts. This is similar to a warm restart, such as by entering the reboot command. The BMC does not reboot itself during this operation.
 - **Power Off System - Immediate**— Disconnect power to the appliance immediately, without gracefully shutting down the appliance. The BMC continues to operate normally in this mode to allow the user to remotely power on the appliance. This is the same as pushing the power button until the unit powers off.
 - **Power Off System - Orderly Shutdown**— Gracefully shut down the appliance, and then disconnect power to the appliance. Has the same effect as pressing the power button on the back panel of the appliance for less than four seconds. All operations on the appliance are stopped, no new connections to the client or server are accepted, and all existing connections are closed before the appliance shuts down. The BMC continues to operate normally in this mode to allow the user to remotely power on the appliance. This is the same as entering the shutdown command in the appliance shell.
 - **Power On System**— Turn on the appliance. The BMC does not reboot itself during this operation. This is the same as pushing the power button.
 - **Power Cycle System**— Turn off the appliance, and then turn it back on. The BMC does not reboot itself during this operation. This is the same as pushing the power button until the unit powers off, and then pushing the power button to power on the unit.
3. Click Perform Action.

Performing a power cycle of the BMC

A warm restart, cold restart, or a power cycle of the appliance, using the power button, does not include power cycling the BMC. The BMC runs on standby power directly from the power supply. Therefore, the BMC is not affected by any state of the power button on the appliance. The only way to power cycle the BMC is to remove all power cords from the appliance for 60 seconds.

Performing power control operations on the BMC by using the appliance shell

When performing either a warm or cold restart of the BMC microcontroller, you cannot communicate with the LOM port. Both actions restart the BMC but not the main CPU. To perform a warm restart of LOM from the appliance, type:

```
ipmitool mc reset warm
```

To perform a warm restart remotely from another computer on the network, type:

```
ipmitool -U <bmc_gui_username> -P <bmc_gui_password> -H <bmc IP address> mc reset warm
```

To perform a cold restart of the LOM from the appliance, type:

```
ipmitool mc reset cold
```

To perform a warm restart remotely from another computer on the network, type:

```
ipmitool -U <bmc_gui_username> -P <bmc_gui_password> -H <bmc IP address> mc reset cold
```

Performing a Core Dump

If the appliance fails or becomes unresponsive, you can remotely perform a core dump. This procedure has the same effect as pressing the NMI button on the back panel of the appliance.

To perform a core dump by using the GUI

1. In the Menu bar, click Remote Control.
2. Under Options, click NMI, and then click Initiate NMI.

To perform a core dump remotely from another computer on the network by using the shell

At the shell prompt, type:

```
ipmitool -U <bmc_gui_username> -P <bmc_gui_password> -H <bmc IP address> chassis power diag
```

Restoring the BMC Configuration to Factory Defaults

Jan 31, 2011

You can restore the BMC to its factory-default settings, including deleting the SSL Certificate and SSL key.

To reset the configuration to factory defaults by using the GUI

1. Navigate to Maintenance > Factory Default.
2. Click Restore.

To reset the configuration to factory defaults by using the shell

At the shell prompt, type:

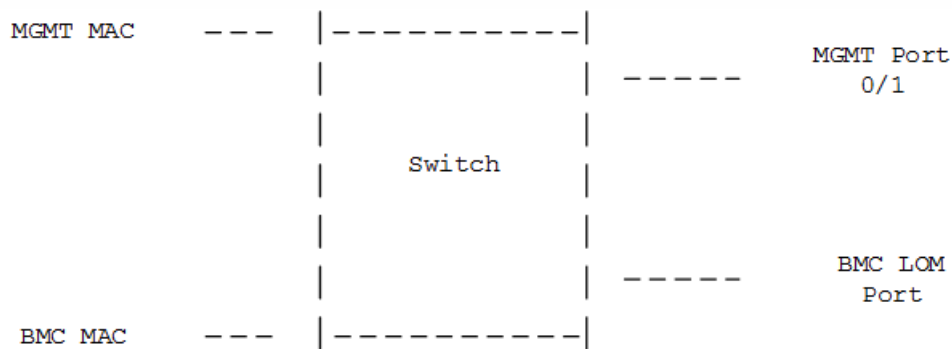
```
ipmitool raw 0x30 0x41 0x1
```

Specifying the Port for IPMI BMC Failover

Jan 31, 2011

With LOM firmware version 3.x or later, the default mode for failover between the dedicated LOM port and the shared LOM/management port is to fail over to the active port. By default, no user configuration is needed other than selecting the port to which to connect the cable. The motherboard has an Ethernet switch between the management MAC and the management port, and between the LOM MAC and the LOM port. The following figure shows the Ethernet switch.

Figure 1. Ethernet Switch



You can set this switch to direct LOM traffic through the dedicated LOM port or through the shared management port. A dedicated LOM port removes the management port as a single point of failure, while a shared LOM/management port reduces the cabling costs.

Using the BIOS POST Code to Detect Errors

Jan 31, 2011

You can read the BIOS POST code by using the LOM GUI or the shell. To interpret the BIOS Beep codes, see https://www.ami.com/support/doc/AMI_Aptio_4.x_Status_Codes_PUB.pdf.

To read the BIOS Post Code by using the LOM GUI

Navigate to Miscellaneous > BIOS Post Snooping.

To read the BIOS Post Code by using the shell

At the prompt, type:

```
ipmitool raw 0x30 0x2a
```

Upgrading the Components of a NetScaler SDX Appliance

May 11, 2015

Upgrading a NetScaler SDX appliance involves upgrading one or more of the SDX components - the Management Service, the XenServer hypervisor, and the NetScaler instances. Based on your requirements, you can choose the component of the NetScaler SDX appliance you want to upgrade. It is generally recommended to upgrade the Management Service first, then the XenServer, then the NetScaler instances (if necessary).

Citrix recommends using the latest version of XenServer supported on the corresponding version of the Management Service. Also, make sure you apply the latest versions of the Supplemental Packs and Hotfixes. See the [Supported Versions](#) table for the recommended Management Service, XenServer, and NetScaler software versions on the NetScaler SDX appliance.

Upgrade Scenarios and Steps

The following table summarizes scenarios and the upgrade steps you must follow to upgrade your NetScaler SDX appliance under each scenario.

Upgrade Type	User Scenarios	Upgrade Steps	Tips
Management Service	<ul style="list-style-type: none"> Upgrading to a later version to enable new NetScaler SDX features. Downgrading to a previous version because of issues with the current version. Upgrading the management service before upgrading the XenServer version. 	<ol style="list-style-type: none"> Check the existing versions running on Management Service and XenServer. See the Supported Versions table. Upgrade the Management Service. 	<ul style="list-style-type: none"> You can upgrade the Management Service without shutting down the NetScaler instances.
XenServer	<p>Upgrading to a later version of XenServer to enable new NetScaler SDX features that are supported on a specific version of XenServer. For example: Provisioning third Party VMs or enabling LACP is possible only if with</p>	<ol style="list-style-type: none"> Check the existing versions running on Management Service and XenServer. See the Supported Versions table to see if the current Management Service version supports the XenServer upgrade. If not, upgrade the Management Service to the appropriate version. 	<ul style="list-style-type: none"> Citrix recommends that you back up the appliance's configuration before upgrading the XenServer. During the upgrade process the NetScaler SDX appliance reboots multiple times, so, you might want to secure a serial console access to the NetScaler SDX appliance. During the upgrade, all the VMs hosted on the appliance are

Upgrade Type	User Scenarios	Upgrade Steps	Tips
	XenServer is running version 6.1.0.	3. Upgrade the XenServer hypervisor.	rebooted. <ul style="list-style-type: none"> • After you upgrade, check the supplemental pack version on the Management Service and be sure to install all the required XenServer hotfixes and supplemental packs if required. • Do not upgrade XenServer using the command line interface.
XenServer Hot Fix	Applying a hotfix when a specific bug is resolved on the XenServer.	<ol style="list-style-type: none"> 1. Check the existing versions running on Management Service and XenServer. 2. Check the Supported Versions table. 3. Check the NetScaler download page for XenServer Hot Fixes and apply any that are available. 	<ul style="list-style-type: none"> • Citrix recommends that you backup the appliance's configuration before applying a XenServer hotfix. • You need not upgrade the XenServer version when you apply a hotfix. • When applying hotfixes on the NetScaler download page, apply them in them in the chronological order.
XenServer Supplemental Pack	<p>Installing a XenServer Supplemental Pack that has a specific NetScaler SDX enhancements.</p> <p>For example, the NetScaler SDX health monitoring feature is supported on XenServer 6.0 with SP 100003 or later.</p>	<ol style="list-style-type: none"> 1. Check the existing versions running on Management Service and XenServer. 2. Check the Supported Versions table. 3. Check the NetScaler download page for XenServer Supplemental Pack and install any that are available. 	<ul style="list-style-type: none"> • Supplemental Packs are version specific. Be sure to apply the correct version for your XenServer version.
NetScaler Instance	Upgrading to a later NetScaler version.	<ol style="list-style-type: none"> 1. Check the existing versions running on Management Service, XenServer, and NetScaler instance. 2. Check the Supported Versions table. 3. Upgrade the NetScaler instance. 	<ul style="list-style-type: none"> • If you are looking for a particular enhancement, make sure that you are running the latest NetScaler version and check the XenServer and Management Service version requirements for that enhancement.

Upgrading the Management Service

Sep 27, 2013

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.

Upgrading the Management Service

Apr 18, 2015

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.

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 Management Service to a Later Version

Sep 06, 2015

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

Oct 18, 2013

You need to upgrade to XenServer version 6.1.0 to enable LACP and provisioning of third-party virtual machines (instances). 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.

Upgrading the XenServer Software

Apr 18, 2015

You need to upgrade to XenServer version 6.1.0 to enable LACP and provisioning of third-party virtual machines (instances). 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.

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.

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.

Upgrading the Software

Sep 06, 2015

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

Mar 21, 2012

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

Jun 25, 2013

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.

Upgrading a NetScaler Instance

Oct 07, 2013

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.

Upgrading a NetScaler Instance

Apr 18, 2015

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.

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. In the details pane, select the instance, and then in the Actions drop down menu, click Upgrade.
- 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 Software Image, 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.

Upgrading NetScaler VPX Instances

Sep 06, 2015

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. In the details pane, select the instance, and then in the Actions drop down menu, click Upgrade.
- 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 Software Image, 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 and Monitoring the NetScaler SDX Appliance

Apr 18, 2015

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.

If a task that you need to perform is not described below, see the list of tasks at the left.

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

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, click **System**. In the **System** pane, under the **Setup Appliance** group, click **Network Configuration** and enter the details in the wizard.

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.

To change the password of the default user account, click **System** > **User Administration** > **Users**. Select a user and click **Edit** to change the password.

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, click **System** and in the **System Settings** group, click **Change Time Zone**.

Modifying the Hostname of the Appliance

You can change the hostname of the Management Service.

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, click **System > Interfaces**. Select an interface and click **VLAN Filter** and enter the details to enable VLAN filtering.

Configuring Clock Synchronization

Updated: 2014-08-24

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

Updated: 2013-10-07

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 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 Instances

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

Available 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

Updated: 2013-10-07

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.

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.

SSL certificates and keys for NetScaler instances

Separate views of SSL certificates and keys for NetScaler instances provide enhanced usability. You can use a new Management Service node, SSL Certificate Files, to upload and manage the SSL certificates and corresponding public and private key pairs that can be installed on NetScaler instances.

To access the SSL certificates and keys for NetScaler instances, navigate to Configuration > NetScaler > SSL Certificate Files.

Name	Last Modified	Size
test1.cert	2014-03-12 03:57:15	973 bytes
test1.cnf	2014-03-12 03:57:15	224 bytes
test2.cert	2014-03-12 03:57:15	973 bytes
test2.cnf	2014-03-12 03:57:15	224 bytes
test3.cert	2014-03-12 03:57:15	973 bytes

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, click Configuration > System and in the System Settings group, click Change System Settings.

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 instances, and then restarts XenServer. When XenServer restarts, it starts all hosted 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.

Changing the Password of the Default User Account

Updated: 2014-08-24

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.

Modifying the Time Zone on the Appliance

Updated: 2014-08-24

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 the Hostname of the Appliance

Updated: 2014-08-24

You can change the hostname of the Management Service.

To modify the hostname, click System and in the System Settings group, click Change Hostname.

To modify the hostname

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under System Settings, click Change Hostname.
3. In the Modify Hostname dialog box, enter a hostname.
4. Click OK.

Managing the RAID disk allocation

Dec 03, 2015

Redundant Array of Independent Disks (RAID) functionality is supported on the following NetScaler SDX appliances:

- NetScaler SDX 22040/22060/22080/22100/22120
- NetScaler SDX 14020/14030/14040/14060/14080/14100

In this document:

- [Managing the RAID Disk Allocation on NetScaler SDX 22040/22060/22080/22100/22120 Appliances](#)
- [Managing the RAID Disk Allocation on NetScaler SDX 14020/14030/14040/14060/14080/14100 Appliances](#)

Managing the RAID Disk Allocation on NetScaler SDX 22040/22060/22080/22100/22120 Appliances

NetScaler SDX 22040/22060/22080/22100/22120 appliances now include a Redundant Array of Independent Disks (RAID) controller, which can support up to eight physical disks. Multiple disks provide not only performance gains, but also enhanced reliability. Reliability is especially important for a NetScaler SDX appliance, because the appliance hosts a large number of virtual machines, and a disk failure affects multiple virtual machines. The RAID controller on the Management Service supports the RAID 1 configuration, which implements disk mirroring. That is, two disks maintain the same data. If a disk in the RAID 1 array fails, its mirror immediately supplies all needed data.

RAID 1 disk mirroring combines two physical drives in one logical drive. The usable capacity of a logical drive is equivalent to the capacity of one of its physical drives. Combining two 1-terabyte drives, for example, creates a single logical drive with a total usable capacity of 1-terabyte. This combination of drives appears to the appliance as a single logical drive.

The SDX appliance is shipped with a configuration that includes logical drive 0, which is allocated for the Management Service and XenServer, and logical drive 1, which is allocated for NetScaler instances that you will provision. To use additional physical drives, you have to create new logical drives.

Viewing Drive Properties and Operations

A NetScaler SDX appliance supports a maximum of eight physical-drive slots, that is, a pair of four slots on each side of the appliance. You can insert physical drives into the slots. Before you can use a physical drive, you must make it part of a logical drive needs.

In the Management Service, the **Configuration > System > RAID** screen includes tabs for logical drives, physical drives, and storage repositories.

Logical Drives

On the **Configuration > System > RAID > Logical Drives** tab, you can view the name, state, size, of each logical drive, and information about its component physical drives. The following table describes the states of the virtual drive.

State	Description
Optimal	The virtual drive operating condition is good. All configured drives are online.
Degraded	The virtual drive operating condition is not optimal. One of the configured drives has failed or is

offline.

Failed	The virtual drive has failed.
Offline	The virtual drive is not available to the RAID controller.

You can also view the details the physical drives associated with the logical drive by selecting the logical drive and clicking Show Physical Drive.

To create a new logical drive

1. Navigate to **Configuration > System > RAID**, and select the Logical Drives tab.
2. Click Add.
3. In the Create Logical Disk dialog box, select two slots that contain operational physical drives, and then click Create.

Physical Drives

A NetScaler SDX appliance supports a maximum of eight physical slots, that is, a pair of four slots on each side of the appliance. On the **Configuration > System > RAID > Physical Drives** tab, you can view the following information:

- **Slot**—Physical slot associated with the physical drive.
- **Size**—Size of the physical drive.
- **Firmware State**—State of the firmware. Possible Values:
 - Online, spun up—Physical drive is up and is being controlled by RAID.
 - Unconfigured (good)—Physical drive is in good condition and can be added as a part of the logical drive pair.
 - Unconfigured (bad)—Physical drive is not in good condition and cannot be added as part of a logical drive.
- **Foreign State**— Indicates if the disk is empty.
- **Logical Drive**— Associated logical drive.

In the Physical Drives pane, you can perform the following actions on the physical drives:

- **Initialize**— Initialize the disk. You can initialize the physical drive if it is not in good state and needs to be added as a part of logical drive pair.
- **Rebuild**— Initiate a rebuild of the drive. When a drive in a drive group fails, you can rebuild the drive by re-creating the data that was stored on the drive before it failed. The RAID controller re-creates the data stored on the other drives in the drive group.
- **Locate**— Locate the drive on the appliance, indicated by causing the Drive Activity LED associated with the drive to blink.
- **Stop Locate**— Stop locating the drive on the appliance.

Prepare to Remove— Deactivate the selected physical drive so that it can be removed.

Storage Repository

On the **Configuration > System > RAID > Storage Repository** tab, you can view the status of storage repositories on NetScaler SDX appliance. You can also view information about a storage-repository drive that is not attached, and you can remove such a drive by selecting the it and then clicking **Remove**. The Storage Repository tab displays the following information about each storage repository:

- **Name**—Name of the storage repository drive.
- **Is Drive Attached**—Whether the storage repository is attached or not. If the drive is not attached, you can click **Remove** to delete.
- **Size**—Size of the storage repository.
- **Utilized**—Amount of storage-repository space in use.

Adding One Additional Logical Drive to the SDX 22000 Appliance

To add an additional logical drive to the SDX 22000 platform:

1. Log on to the Management Service.
2. Navigate to **Configuration > System > RAID**.
3. On the back of the SDX 22000 appliance, insert the two blank SSDs in slot numbers 4 and 5. You can add the SSDs in a running system.
Note: Make sure that the SSDs are Citrix certified.
4. In the Management Service, navigate to Configuration > System > RAID and click the Physical Drives tab. You would see the SSDs that you added.
5. Navigate to the Logical Drive tab and click Add.
6. In the Create Logical Disk page:
 1. In the First Slot drop-down list, select 4.
 2. In the Second Slot drop-down list, select 5.
 3. Click Create.

Note: In Management Service, the slot number begins with zero. So the slot numbering in Management Service differs from the slot numbering on the physical appliance.

The logical drive is created and is listed under the Logical Drive tab. Click the refresh icon to update the order of the logical drives.

Adding Second Additional Logical Drive on the SDX 22000 Appliance

To add another logical drive, insert the SSDs in slot numbers 6 and 7. In the Create Logical Disk page, select 6 from the First Slot drop-down list and select 7 from the Second Slot drop-down list.

Replacing a Defective SSD Drive with a Blank SSD Drive

To replace a defective SSD drive with a blank SSD drive:

1. Navigate to Configuration > System > RAID.
2. On the Physical Drives tab, select the defective drive that you want to replace.
3. Click Prepare to Remove to remove the drive.
4. Click the refresh icon to refresh the list of physical drives.
5. Physically remove the defective drive from the slot.
6. Insert the new Citrix verified SSD in the slot from where you removed the defective SSD.
7. In the Management Service, navigate to Configuration > System > RAID. The new SSD is listed in the Physical Drives section. The drive rebuild process starts automatically.

Click the refresh icon to check the status of the rebuild process. When the rebuild process is complete, you can see Online, Spun Up status in the Firmware State column.

Managing the RAID Disk Allocation on NetScaler SDX 14020/14030/14040/14060/14080/14100 Appliances

NetScaler SDX 14020/14030/14060/14060/14080/140100 appliances support RAID managed by the software. Multiple disks provide not only performance gains, but also enhanced reliability. Reliability is especially important for a NetScaler SDX appliance, because the appliance hosts a large number of virtual machines, and a disk failure affects multiple virtual machines. The NetScaler SDX appliance supports RAID 1 configuration, which implements disk mirroring. That is, two disks maintain the same data. If a disk in the RAID 1 array fails, its mirror immediately supplies all the needed data.

RAID 1 disk mirroring combines two physical drives in one logical drive. The usable capacity of a logical drive is equivalent to the capacity of one of its physical drives. Combining two 279 GB drives, for example, creates a single logical drive with a total usable capacity of 279 GB. This combination of drives appears to the appliance as a single logical drive.

The SDX appliance in its default configuration is shipped with four disk slots populated with solid-state drives (SSDs). The NetScaler SDX 14040 appliance is shipped with six slots populated with SSDs and NetScaler SDX 14060/14080 appliances are shipped with all eight slots populated with SSDs. It includes the logical drive 0, which is allocated for the Management Service and XenServer, and logical drive 1, which is allocated for NetScaler instances that a user will provision. Disks in slots 1 and 2 create a RAID 1 pair for logical drive 0. Similarly, disks in slots 3 and 4 create a RAID 1 pair for logical drive 1. For additional storage as dictated by model number, license and capacity requirements, you can create additional new logical drives. This requires populating physical drives to form RAID 1 pairs in slots 5 and 6, and/or slots 7 and 8.

Viewing Drive Properties and Operations

The NetScaler SDX 14000 appliance supports a maximum of eight physical-drive slots. You can insert physical drives into the slots. Before you can use a physical drive, you must make it part of a logical drive.

In the Management Service, the **Configuration > System > RAID** screen includes tabs for storage repositories, logical drives, and physical drives.

Storage Repository

On the **Configuration > System > RAID > Storage Repository** tab, you can view the status of storage repositories on the NetScaler SDX appliance. The Storage Repository tab displays the following information about each storage repository:

- **Name.** Name of the storage repository drive.
- **Size.** Size of the storage repository.
- **Utilized.** Amount of storage-repository space in use.

Logical Drives

On the **Configuration > System > RAID > Logical Drives** tab, you can view the name, state, size of each logical drive, and information about its component physical drives. The following table describes the states of the logical drive.

State	Description
Degraded	The logical drive operating condition is not optimal. One of the configured drives has failed or is offline.
Failed	The logical drive has failed.

Active	The logical drive is fully active, disk I/O and/or resync can be happening.
Clean	The logical drive is active, but does not have any pending write operations.
Recovering	All data on the logical drive is being written from the running array to fill up a new disk with all the relevant data.
Resync	Data on the array is being synchronized from the running array. Data that is not in sync with the running array is added to this array.

The RAID state of a logical drive at times may reflect a combination of above states as below:

clean, degraded

Applies to a degraded RAID 1 where one of the drives has failed or is offline

active, degraded

Applies to a degraded RAID 1 where one of the drives has failed or is offline

active, degraded, resyncing

Applies to a degraded RAID 1, where data on both the drives is in the process of being synchronized.

clean, degraded, recovering

Applies to a degraded RAID 1, where a new drive is being filled up with all the relevant data.

You can also view the details of the physical drives associated with the logical drive by selecting the logical drive and clicking **Show Physical Drives**.

To create a new logical drive

1. Navigate to **Configuration > System > RAID**, and select the Logical Drives tab.
2. Select **md_d2** for **Slot5, Slot6** or **md_d3** for **Slot7, Slot8**.
3. Click **Create**.
4. In the **Create Logical Disk** dialog box, you can select the **Force Clean Physical Disks** option to erase any existing RAID metadata on the drives.
5. Click **Create**.

Physical Drives

Navigate to **Configuration > System > RAID > Physical Drives** tab, to view the following information:

- **Slot** - Physical slot associated with the physical drive.

- **State** - Indicates if a physical drive is present on the appliance.
 - Present** - Physical drive is present on the appliance.
 - Not Present** - It means either the physical drive is absent on the appliance, or it has been deactivated so that it can be removed.
- **Size** - Size of the physical drive.
- **RAID State** - Raid state of the physical drives
 - active, sync - Physical drive in good condition in sync with pending writes
 - clean, sync - Physical drive in good condition in sync with no pending writes
 - spare, rebuilding - A new physical drive is being filled up with relevant data
 - faulty - Physical drive in a faulty state
- **Logical Drive** - Associated logical drive.

In the Physical Drives pane, you can perform the following actions on the physical drives:

- **Rebuild** - Initiate a rebuild of the drive. When a drive in RAID 1 fails, you can rebuild the RAID 1 pair, by providing a new Citrix certified disk and selecting this option.
- **Locate** - Locate the drive on the appliance. Once the drive is located, the activity LED associated with the drive starts to blink.
- **Stop Locate** - Stop locating the drive on the appliance.
- **Prepare to Remove** - Deactivate the selected physical drive so that it can be removed.

Creating the md_d2 Logical Drive on the SDX 14020/14030 Appliance

To add an additional logical drive to the SDX 14020/14030 appliance:

1. On the back of the SDX appliance, insert the two blank SSDs of same capacity in slot numbers 5 and 6. You can add the SSDs in a running system.
 - Note:** Make sure that the SSDs are Citrix certified.
2. In the Management Service, navigate to Configuration > System > RAID and click the Physical Drives tab. You can see the SSDs that you added.
3. Navigate to the Logical Drives tab.
4. Select the md_d2 logical drive.
5. Click Create.
6. In the Create Logical Disk dialog box, you can select the Force Clean Physical Disks option to erase any existing RAID metadata on the drives. The drive is considered as a foreign drive if it came from another RAID setup, or has old RAID metadata that needs to be erased.
7. Click Create. The logical drive md_d2 is created and is listed under the Logical Drives tab.

Note: The md_d2 logical drive is automatically created on the SDX 14040/14060/14080/14100 appliances.

Creating the md_d3 Logical Drive on the SDX 14020/14030/14040 Appliance

To add the md_d3 logical drive, insert the SSDs in slots 7 and 8 at the back of the appliance and follow the instructions in Creating the md_d2 Logical Drive on the SDX 14020/14030 Appliance.

The logical drive md_d3 is created and is listed under the Logical Drives tab.

Note: The md_d3 logical drive is automatically created on the SDX 14060/14080/14100 appliances.

Replacing a Failed or Defective SSD with a Blank SSD

To replace a defective SSD with a blank SSD:

1. In the Management Service, navigate to **Configuration > System > RAID**.
2. On the **Physical Drives** tab, select the defective drive that you want to replace.
3. Click **Prepare to Remove** to trigger the removal of the drive. The state of the drive should now appear as Not Present.
4. Physically remove the defective drive from the slot.
5. Insert the new Citrix certified SSD in the slot from where you removed the defective SSD.
6. On the Physical Drives tab, click the refresh icon to refresh the list of physical drives. The state of the drive should now appear as Present.
7. Select the drive and click the Rebuild option.
8. In the Rebuild Physical Drive dialog box, you can select the Force Clean option to erase any existing RAID metadata on the drive. The drive is considered as a foreign drive if it came from another RAID setup, or has old RAID metadata that needs to be erased.
9. Click OK. The state of the drive should now appear as spare, rebuilding.

Replacing a Failed RAID Logical Drive with Two Blank SSDs

If both the SSDs that form a RAID1 pair fail, you must first delete the NetScaler VPX instances hosted on the storage repository associated with the failed SSDs, delete the logical drive, replace both the failed SSDs with new Citrix certified SSDs, and create the logical drive again.

To replace two failed SSDs

1. In the Management Service, on the Dashboard tab, in the right-side panel, under Storage Repositories, click Details to identify the storage repository associated with the failed SSDs.
For example, if SSDs in slot 5 and slot 6 have failed, the storage repository associated with these SSDs is VPX-SR-2.
2. Navigate to Configuration > NetScaler > Instances, select a VPX instance, click the drop down arrow, and see the Disk Allocation column to check if that VPX instance is hosted on the storage repository associated with the failed SSDs. If yes, delete the VPX instance. Delete all VPX instances hosted on that storage repository.
3. Navigate to Configuration > System > RAID > Logical Drives, and delete the logical drive associated with the failed SSDs.
For example, if SSDs in slot 5 and slot 6 have failed, you must select the logical drive md_d2, and click Delete.
4. Replace the failed SSDs with new Citrix certified SSDs in the corresponding pair of slots.
5. Create the logical drive associated with the replaced SSDs. For example, select md_d2, and click Create.
The logical drive with the replaced SSDs is created and is ready for use. You can now provision VPX instances that you deleted earlier.

NetScaler SDX Licensing Overview

Apr 18, 2015

The process of allocating your licenses has been greatly simplified. The new licensing framework allows you to focus on getting maximum value from Citrix products.

In the Management Service configuration utility (GUI), you can use your hardware serial number (HSN) or your license activation code (LAC) to allocate your licenses. Alternatively, if a license is already present on your local computer, you can upload it to the appliance.

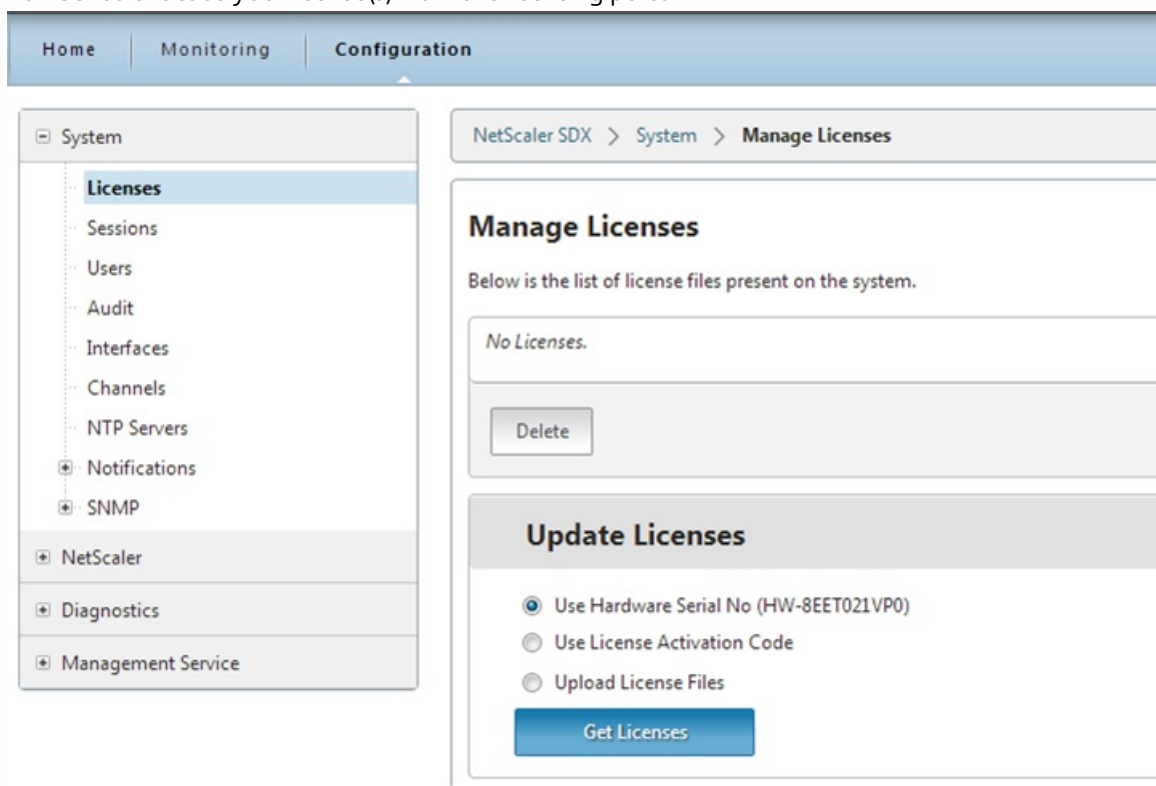
For all other functionality, such as returning or reallocating your license, you must use the licensing portal. Optionally, you can still use the licensing portal for license allocation. .

If your license is already linked to your hardware, the license allocation process can use the hardware serial number. Otherwise, you must type the license activation code (LAC).

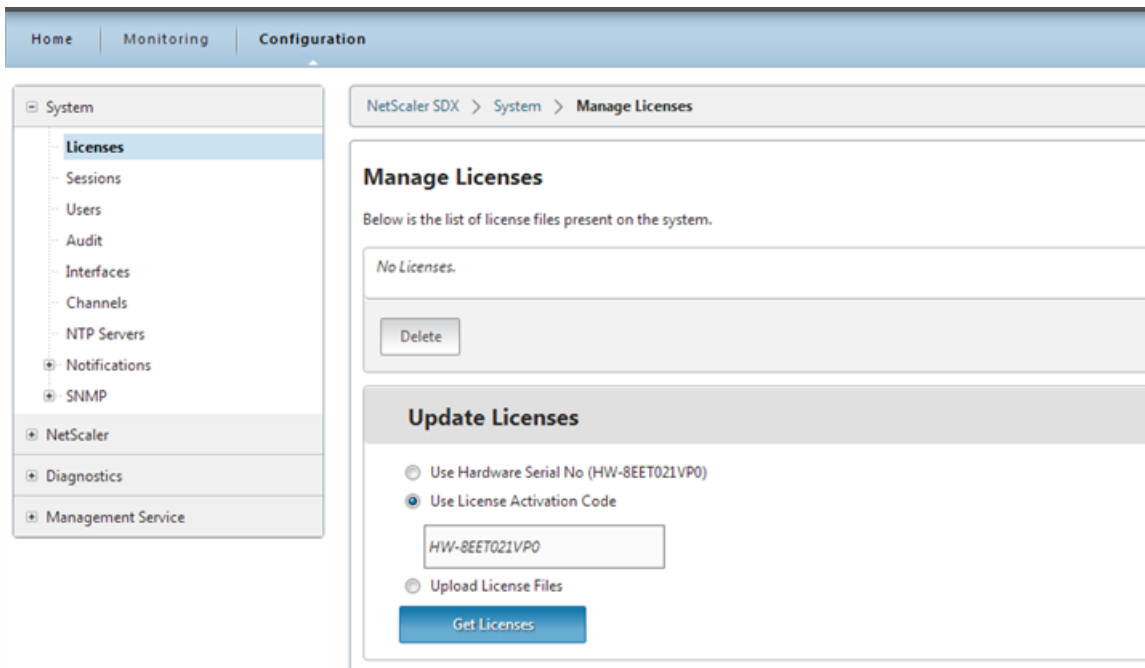
Note: You do not need to restart your appliance after you have allocated the license.

To allocate your license by using the hardware serial number or the license activation code

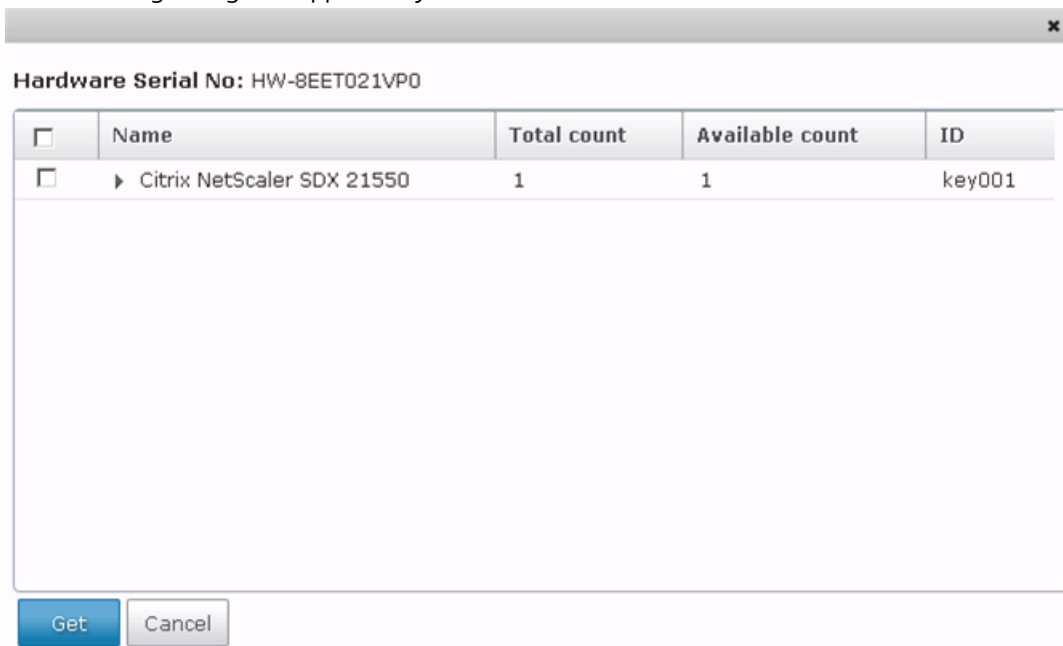
1. In a web browser, type the IP address of your NetScaler SDX appliance.
2. In User Name and Password, type the administrator credentials.
3. On the Configuration tab, navigate to System > Licenses.
4. In the details pane, under Update Licenses, select one of the following options:
 - **Use Hardware Serial Number**—The software internally fetches the serial number of your appliance and uses this number to allocate your license(s) from the licensing portal.



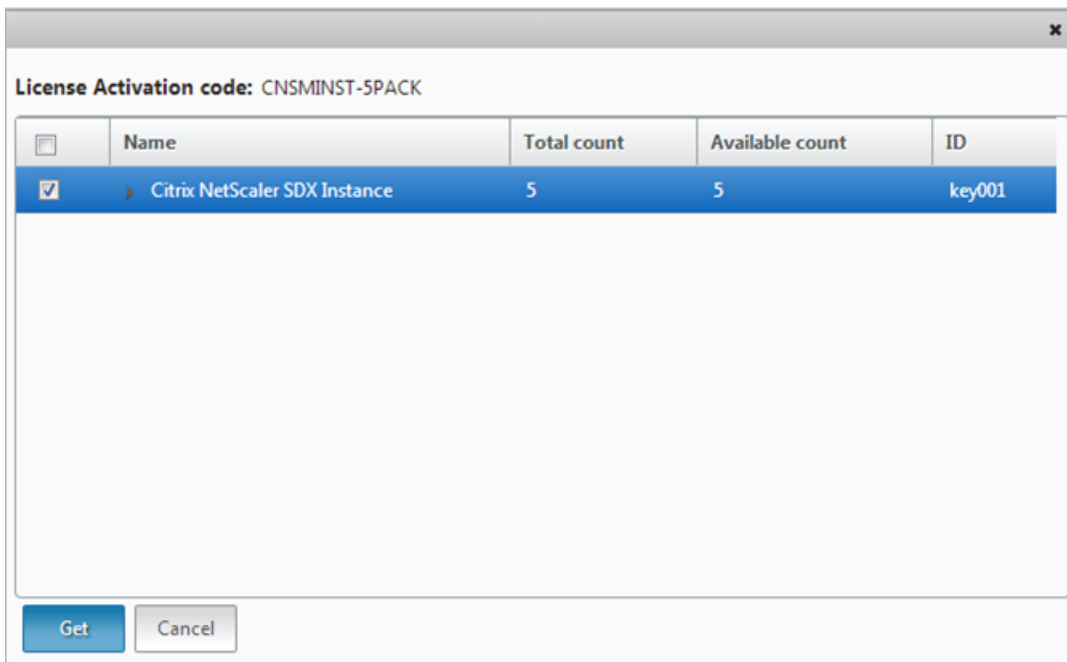
- **Use License Activation Code**—Citrix emails the LAC for the license that you purchased. Enter the LAC in the text box.



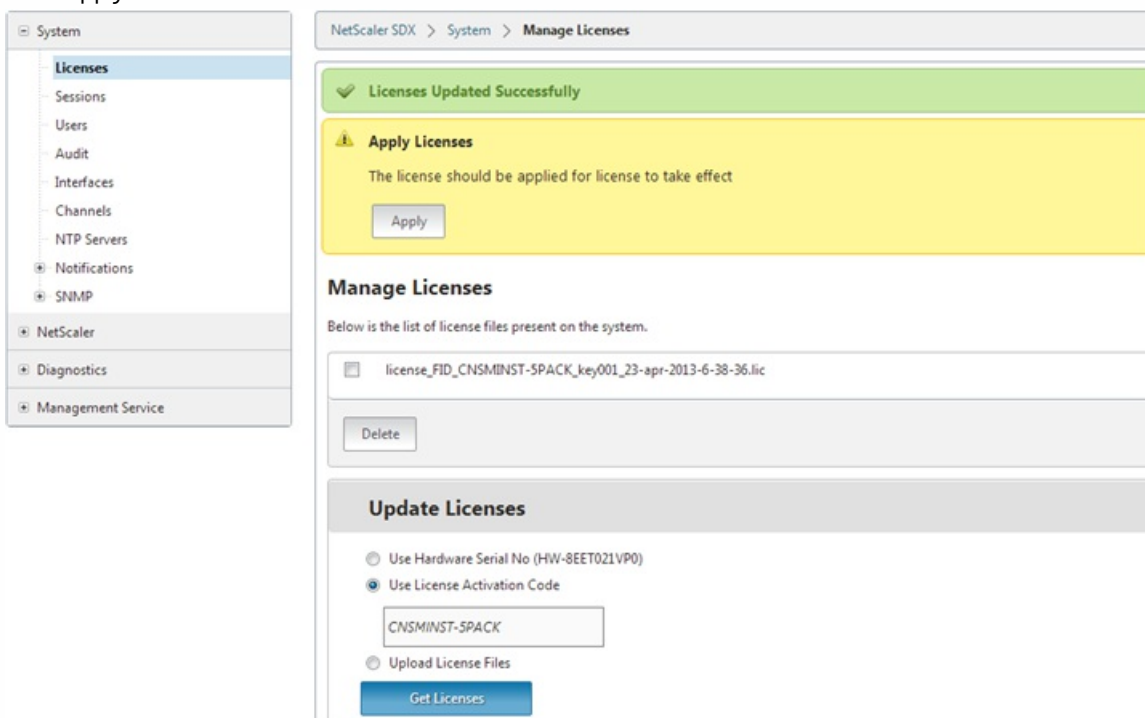
5. Click Get Licenses. Depending on the option that you selected one of the following dialog boxes appears.
- The following dialog box appears if you selected Hardware Serial Number.



- The following dialog box appears if you selected License Activation Code.



6. Select the license that you want to allocate, and then click Get.
7. Click Apply for the license to take effect.



Uploading your License

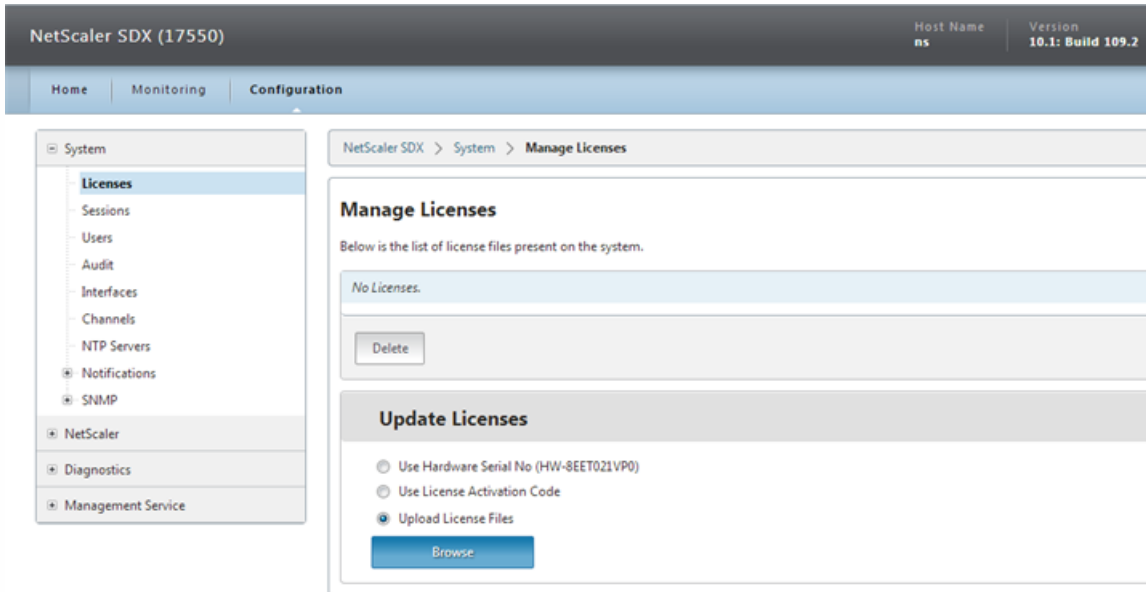
Updated: 2014-08-24

If you downloaded your license file to your local computer by accessing the licensing portal, you must upload the license to the appliance.

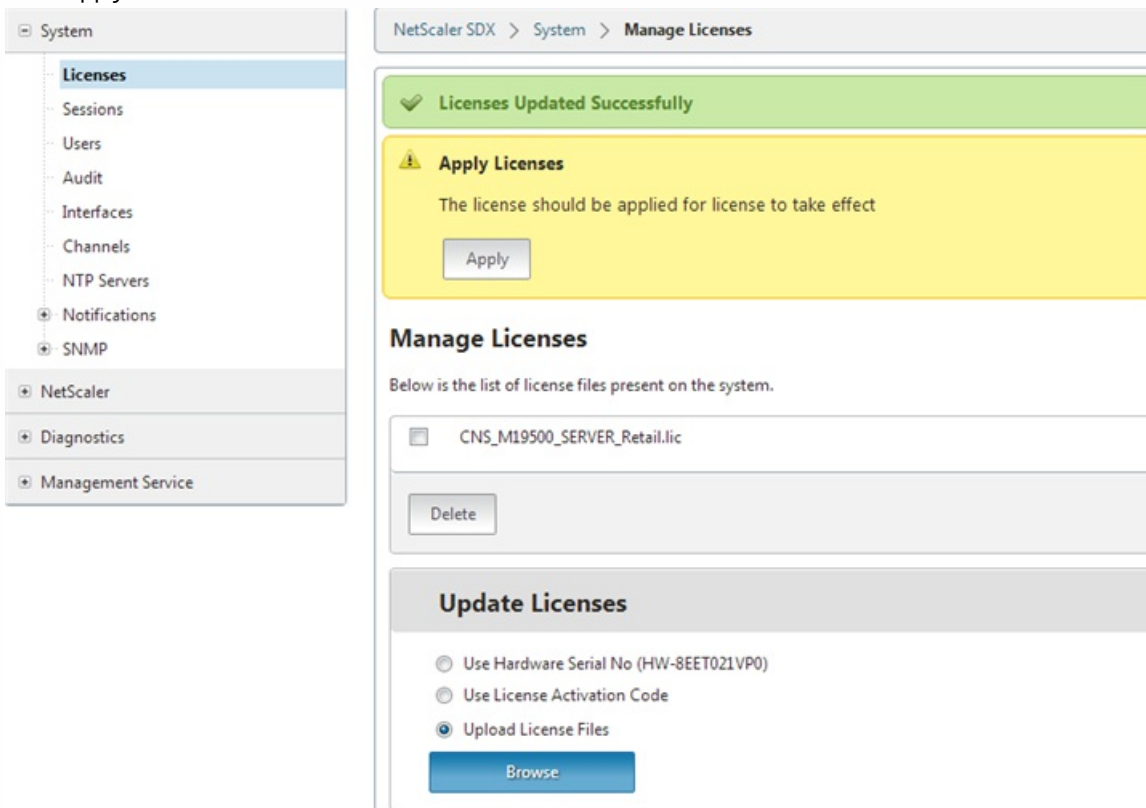
To upload a license file

1. In a web browser, type the IP address of your NetScaler SDX appliance.

2. In User Name and Password, type the administrator credentials.
3. On the Configuration tab, navigate to System > Licenses.
4. In the details pane, click Update Licenses, and then select Upload License Files.



5. Click Browse. Navigate to the location of the license files, select the license file, and then click Open.
6. Click Apply for the license to take effect.



Managing Interfaces

May 24, 2016

In the management service's Interfaces pane, in addition to configuring transmission settings for each interface, you can display the mapping of the virtual interfaces on the VPX instances to the NetScaler SDX appliance, and assign MAC addresses to interfaces.

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

In the list of Interfaces in the Interfaces pane, in the State column, UP indicates that the interface is receiving traffic normally. 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 ModifyEdit.
 3. In the Modify Interface window, under Link Speed and Flow Control specify values for the following parameters:
 - Auto Negotiation*— Enable auto-negotiation. Possible values: ON, OFF. Default: OFF.
 - Speed*— Ethernet speed for the interface, in Mb/s. Possible values: 10, 100, 1000, and 10000.
 - Duplex*— Type of duplex operation of the interface. Possible values: Full, Half, NONE. Default: NONE.
 - Flow Control Auto Negotiation*— Automatically negotiate flow control parameters. Possible values: ON, OFF. Default: ON
 - Rx Flow Control*— Enable Rx flow. Possible values: ON, OFF. Default: ON
 - Tx Flow Control*— EnableTx flow control is enabled. Possible values: ON, OFF. Default: ON
- * 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.

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

Updated: 2015-04-14

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:

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

NetScaler VPX ()		Host Name 10.102.163.15	Version NS10.1: Build 95.2.a.nc, Date: Jan 9 2013, 01:																																				
<div style="display: flex; justify-content: space-between;"> Dashboard Configuration Reporting </div>																																							
<ul style="list-style-type: none"> System Network <ul style="list-style-type: none"> IPs Interfaces Channels Traffic Domains IP Tunnels VLANs Bridge Groups 	<div style="display: flex; justify-content: space-between;"> NetScaler Network Interfaces Refresh </div> <table border="1"> <thead> <tr> <th>Interface</th> <th>Description</th> <th>Alias Name</th> <th>MAC</th> <th>Uptime</th> <th>Down</th> </tr> </thead> <tbody> <tr> <td>▶ 0/1</td> <td>(NetScaler Virtual Interface, PF 0/1) #3</td> <td></td> <td>da:54:0d:af:0c:a5</td> <td>1d 19h 34m 39s</td> <td></td> </tr> <tr> <td>▶ 10/1</td> <td>(10G VF Interface, PF 10/1) #0</td> <td></td> <td>ce:fa:8c:d5:2d:55</td> <td>1d 19h 34m 46s</td> <td></td> </tr> <tr> <td>▶ 10/2</td> <td>(10G VF Interface, PF 10/2) #1</td> <td></td> <td>ba:14:1d:f9:e1:d0</td> <td>1d 19h 34m 46s</td> <td></td> </tr> <tr style="border: 2px solid red;"> <td>▶ 10/3</td> <td>(10G VF Interface, PF 10/4) #2</td> <td></td> <td>6e:b6:f5:21:5d:db</td> <td>1d 18h 5m 53s</td> <td></td> </tr> <tr> <td>▶ LO/1</td> <td>(Netscaler Loopback interface) #4</td> <td></td> <td>da:54:0d:af:0c:a5</td> <td>1d 19h 34m 46s</td> <td></td> </tr> </tbody> </table>			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	
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																																			

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) FctIs(0) Stalls(0) Hangs(0) Muted(0)
Bandwidth thresholds are not set.
```

Assigning a MAC Address to an Interface

Updated: 2014-08-24

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

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.

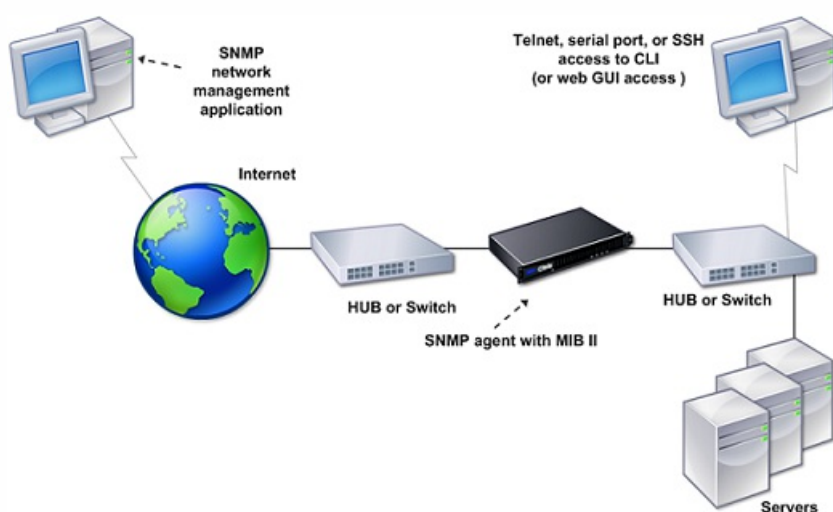
Configuring SNMP on NetScaler SDX Appliances

Apr 18, 2015

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*



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 Configure SNMP Trap Destination 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.

Adding an SNMP Manager Community

You must configure the NetScaler SDX appliance to allow the appropriate SNMP managers to query it. You must also provide the SNMP manager with the required appliance-specific information. For an IPv4 SNMP manager you can specify a host name instead of the manager's IP address. If you do so, you must add a DNS name server that resolves the host name of the SNMP manager to its IP address.

You must configure at least one SNMP manager. If you do not configure an SNMP manager, the appliance does not accept or respond to SNMP queries from any IP address on the network. If you configure one or more SNMP managers, the appliance accepts and responds only to SNMP queries from those specific IP addresses.

To configure an SNMP manager

1. On the Configuration tab, in the navigation pane, expand System, and then expand SNMP.
2. Click Managers.
3. In the details pane, click Add.
4. In the Add SNMP Manager Community dialog box, set the following parameters:
 - **SNMP Manager**—IPv4 address of the SNMP manager. Alternatively, instead of an IPv4 address, you can specify a host name that has been assigned to an SNMP manager. If you do so, you must add a DNS name server that resolves the host name of the SNMP manager to its IP address.
 - **Community**—The SNMP community string. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), at (@), equals (=), colon (:), and underscore (_) characters.
5. Click Add, and then click Close.

Configuring an SNMP Alarm

The appliance provides a predefined set of condition entities called SNMP alarms. When the condition set for an SNMP alarm is met, the appliance generates SNMP trap messages that are sent to the configured trap listeners. For example, when the `deviceAdded` alarm is enabled, a trap message is generated and sent to the trap listener whenever a device (instance) is provisioned on the appliance. You can assign a severity level to an SNMP alarm. When you do so, the corresponding trap messages are assigned that severity level.

Following are the severity levels defined on the appliance, in decreasing order of severity:

- Critical
- Major
- Minor
- Warning
- Informational (default)

For example, if you set a Warning severity level for the SNMP alarm named `deviceAdded`, the trap messages generated when a device is added are assigned with the Warning severity level.

You can also configure an SNMP alarm to log the corresponding trap messages generated whenever the condition on that alarm is met.

To modify a predefined SNMP alarm

1. On the Configuration tab, in the navigation pane, expand System.
2. Expand SNMP, and then click Alarms.
3. In the details pane, select an alarm, and then click Modify.
4. In the Modify SNMP Alarm dialog box, from the Severity list, select a severity level.
5. To enable the alarm, select Enable Alarm.
6. Click OK, and then click Close.

Configuring Syslog Notifications

Aug 25, 2014

SYSLOG is a standard logging protocol. It has two components: the SYSLOG auditing module, which runs on the SDX appliance, and the SYSLOG server, which can run on a remote system. SYSLOG uses user data protocol (UDP) for data transfer.

When you run a SYSLOG server, it connects to the SDX appliance. The appliance then starts sending all the log information to the SYSLOG server, and the server can filter the log entries before storing them in a log file. A SYSLOG server can receive log information from more than one SDX appliance, and an SDX appliance can send log information to more than one SYSLOG server.

The log information that a SYSLOG server collects from an SDX appliance is stored in a log file in the form of messages. These messages typically contain the following information:

- The IP address of the SDX appliance that generated the log message
- A time stamp
- The message type
- The log level (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- The message information

You can use this information to analyze the source of the alert and take corrective action if required. First configure a syslog server that the appliance sends log information to, and then specify the data and time format for recording the log messages.

To configure a Syslog Server

1. Navigate to System > Notifications > Syslog.
2. In the details pane, click Add.
3. In the Add Syslog Server Create Syslog Server dialog box, specify values for the syslog server parameters. For a description of a parameter, hover the mouse over the corresponding field.
4. Click Add, and then click Close.

To configure the syslog parameters

1. Navigate to System > Notifications > Syslog.
2. In the details pane, in the Action list, click Syslog Parameters.
3. In the Modify Syslog Parameters Configure Syslog Parameters dialog box, specify the date and time format.
4. Click OK, and then click Close.

Configuring Mail Notifications

Aug 25, 2014

You must configure an SMTP server to receive an email message each time an alert is raised. First configure an SMTP server, and then configure a mail profile. In the mail profile, use commas to separate the addresses of the recipients.

To configure an SMTP server

1. Navigate to System > Notifications > Mail.
2. In the details pane, click SMTP Server, and then click Add.
3. In the Add SMTP Server dialog box, specify values for the server parameters. For a description of a parameter, hover the mouse over the corresponding field.
4. Click Create, and then click Close.

To configure a mail profile

1. Navigate to System > Notifications > Mail.
2. In the details pane, click Mail Profile, and then click Add.
3. In the Create Mail Profile dialog boxpage, specify values for the mail profile parameters. For a description of a parameter, hover the mouse over the corresponding field.
4. Click Create, and then click Close.

Configuring SMS Notifications

Aug 25, 2014

You must configure a short message service (SMS) server to receive an SMS message each time an alert is raised. First configure an SMS server, and then configure an SMS profile. In the SMS profile, use commas to separate the addresses of the recipients.

To configure an SMS server

1. Navigate to System > Notifications > SMS.
2. In the details pane, click SMS Server, and then click Add.
3. In the Add SMS Server dialog box, specify values for the SMS server parameters. The values for these parameters are provided by the vendor.
4. Click Create, and then click Close.

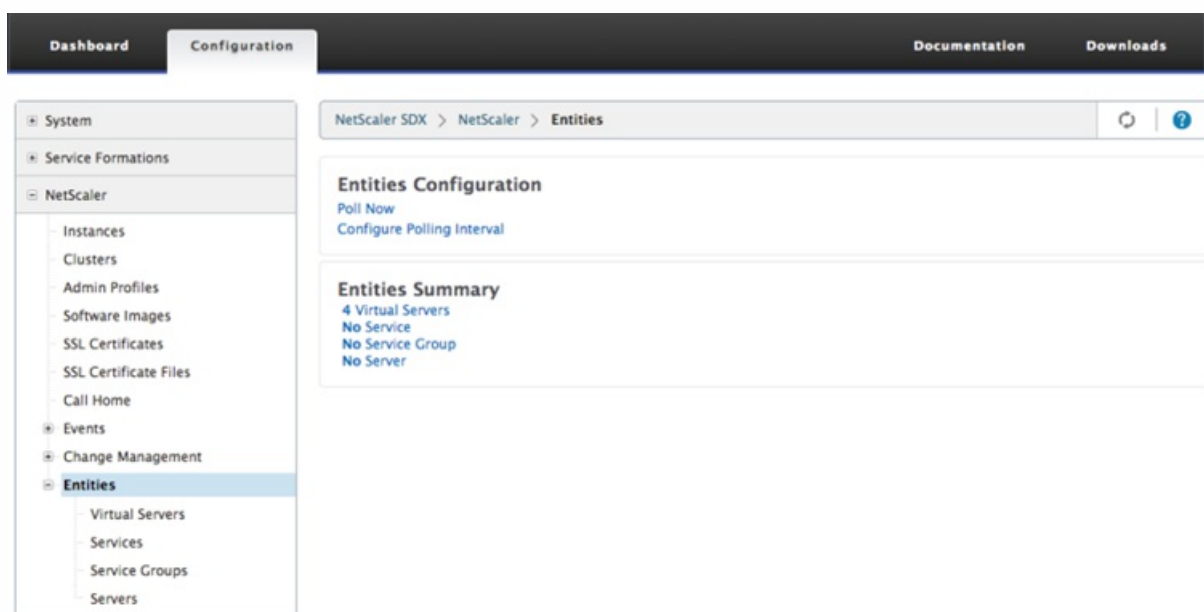
To configure an SMS profile

1. Navigate to System > Notifications > SMS.
2. In the details pane, click SMS Profile, and then click Add.
3. In the Create SMS ProfileCreate SMS Distribution List dialog box, specify values for the mail profile parameters. For a description of a parameter, hover the mouse over the corresponding field.
4. Click Create, and then click Close.

Monitoring and Managing the Real-Time Status of Entities Configured on NetScaler Devices

Apr 09, 2014

Use NetScaler SDX to monitor and manage the states of virtual servers, services, service groups, and servers across the NetScaler virtual appliances hosted on SDX. You can monitor values, such as the health of a virtual server and the time elapsed since the last state change of a service or service group. This gives you visibility into the real-time status of the entities and makes management of these entities easy when you have a large number of entities configured on your NetScaler instances.



Viewing the Status of Virtual Servers

You can monitor the real-time values of the state and health of a virtual server. You can also view the attributes of a virtual server, such as name, IP address, and type of virtual server.

To view the status of a virtual server

1. On the Configuration tab, in the navigation pane, click NetScaler > Entities > Virtual Servers.
2. In the right pane, under Virtual Servers, view the following statistics:
 - Device Name— Name of the NetScaler VPX on which the virtual server is configured.
 - Name— Name of the virtual server.
 - Protocol— Service type of the virtual server. For example, HTTP, TCP, and SSL.
 - Effective State— Effective state of the virtual server, based on the state of the backup vservers. For example, UP, DOWN, or OUT OF SERVICE.
 - State— Current state of the virtual server. For example, UP, DOWN, or OUT OF SERVICE.
 - Health— Percentage of services that are in the UP state and are bound to the virtual server. The following formula is used to calculate the health percentage: $(\text{Number of bound UP services} * 100) / \text{Total bound services}$
 - IP Address— IP address of the virtual server. Clients send connection requests to this IP address.
 - Port— Port on which the virtual server listens for client connections.
 - Last State Change— Elapsed time (in days, hours, minutes, and seconds) since the last change in the state of the virtual server, that is, the duration of time for which the virtual server has been in the current state. This information is

available only for virtual servers configured on NetScaler release 9.0 and later.

NetScaler SDX > NetScaler > Entities > Virtual Servers

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

Viewing Services and Service Groups Bound to a Virtual Server

You can monitor the real-time status of the services and service groups bound to a virtual server. This lets you check the state of the services that might cause the health percentage of a virtual server to become low, so that you can take appropriate action.

To view the services and service groups bound to a virtual server

1. On the Configuration tab, in the left pane, click NetScaler > Entities > Virtual Servers.
2. In the details pane, under Virtual Servers, click the name of the virtual server for which you want to display the bound services and service groups, and under Actions, click Bound Services or Bound Services Groups. Alternatively, right-click the name of the virtual server, and then click Bound Services or Bound Services Groups.

NetScaler SDX > NetScaler > Entities > Virtual Servers

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

Viewing the Status of Services

You can monitor the real-time values of the state of a service and the duration for which the service has been in the current state.

To view the status of virtual servers

1. On the Configuration tab, in the navigation pane, click NetScaler > Entities > Service.
2. In the details pane, under Services, view the following statistics:

- Device Name—Name of the device on which the service is configured.
- Name—Name of the service.
- Protocol—Service type, which determines the behavior of the service. For example, HTTP, TCP, UDP, or SSL.
- State—Current state of the service. For example, UP, DOWN, or OUT OF SERVICE.
- IP Address—IP address of the service.
- Port—Port on which the service listens.
- Last State Change—Elapsed time (in days, hours, minutes, and seconds) since the last change in the state of the service, that is, the duration of time for which the service has been in the current state.

Viewing the Virtual Servers to which a Service is Bound

You can view the virtual servers to which a service is bound and monitor the real-time status of the virtual servers.

To view the virtual servers to which a service is bound

1. On the Configuration tab, in the navigation pane, click NetScaler > Entities > Service.
2. In the details pane, under Services, click the name of the service for which you want to view the bound virtual servers. Then from the Action menu, select Bound Virtual Servers. Alternatively, right-click the service, and then click Bound Virtual Servers.

Name	Protocol	State	IP Address	Port	Last State Change	
ns2(10.102.163.5)	s100	HTTP	Up	172.16.200.100	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s101	HTTP	Up	172.16.200.101	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s102	HTTP	Up	172.16.200.102	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s103	HTTP	Up	172.16.200.103	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s104	HTTP	Up	172.16.200.104	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s105	HTTP	Up	172.16.200.105	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s106	HTTP	Up	172.16.200.106	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s107	HTTP	Up	172.16.200.107	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s108	HTTP	Up	172.16.200.108	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s109	HTTP	Up	172.16.200.109	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	s110	HTTP	Up	172.16.200.110	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	s100	HTTP	Up	172.16.200.100	80	Mon, 10 Mar 2014 17:14:36 GMT

Viewing the Status of Service Groups

You can monitor the real-time state of a service group member from the NetScaler SDX interface.

To view the status of service groups

1. On the Configuration tab, in the navigation pane, click NetScaler > Entities > Service Groups.
2. In the details pane, under Service Groups, view the following statistics:
 - Device Name—Name of the device on which the service group is configured.
 - Name—Name of the service group.
 - IP Address—IP address of each service that is a member of the service group.
 - Port—Ports on which the service group members listen .
 - Protocol—Service type, which determines the behavior of the service group. For example, HTTP, TCP, UDP, or SSL.
 - Effective State—Effective state of the virtual server group, based on the state of the backup virtual servers. For example, UP, DOWN, or OUT OF SERVICE
 - State—Effective state of the service group, which is based on the state of the member of the service group. For example, UP, DOWN, or OUT OF SERVICE.
 - Last State Change—Elapsed time (in days, hours, minutes, and seconds) since the last change in the state of the

service group member, that is, the duration of time for which the service group member has been in the current state. This information is available only for service group members configured on NetScaler release 9.0 and later.

Viewing the Virtual Servers to which a Service is Bound

You can view the virtual servers to which a service is bound and monitor the real-time status of the virtual servers.

To view the virtual servers to which the service is bound

1. On the Configuration tab, in the left pane, click NetScaler > Entities > Servers.
2. In the right pane, under Servers, select the server from the list, and under Actions menu, click Bound Virtual Services. Alternately, right-click the service and click Bound Virtual Servers.

Viewing the Status of Servers

You can monitor and manage the states of servers across the NetScaler instances. This gives you visibility into the real-time status of the servers and makes management of these servers easy when you have a large number of servers.

To view the status of servers

1. On the Configuration tab, in the navigation pane, click NetScaler > Entities > Servers.
2. In the details pane, under Servers, view the following statistics:
 - Device Name: Specifies the name of the device on which the server is configured.
 - Name: Specifies the name of the server.
 - IP Address: Specifies the IP address of the server. Clients send connection requests to this IP address.
 - State: Specifies the current state of the server. For example, UP, DOWN, and OUT OF SERVICE.
 - Last State Change: Specifies the time elapsed (in days, hours, minutes, and seconds) since the last change in the state of the server, that is, the duration of time for which the server is in the current state.

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

Configuring the Polling Interval

You can set the time interval for which you want the NetScaler SDX appliance to poll the real-time values of the virtual servers, services, service groups, and servers. By default, the appliance polls the values every 30 minutes.

To configure the polling interval for virtual servers, services, service groups, and Servers.

1. On the Configuration tab, click NetScaler > Entities, and in the right pane, click Configure Polling Interval.
2. In the Configure Polling Interval dialog box, type the number of minutes you want to set as the time interval for which NetScaler SDX must poll the entity value. Minimum value of the polling interval is 30 minutes. Click OK.

Monitoring and Managing Events Generated on NetScaler Instances

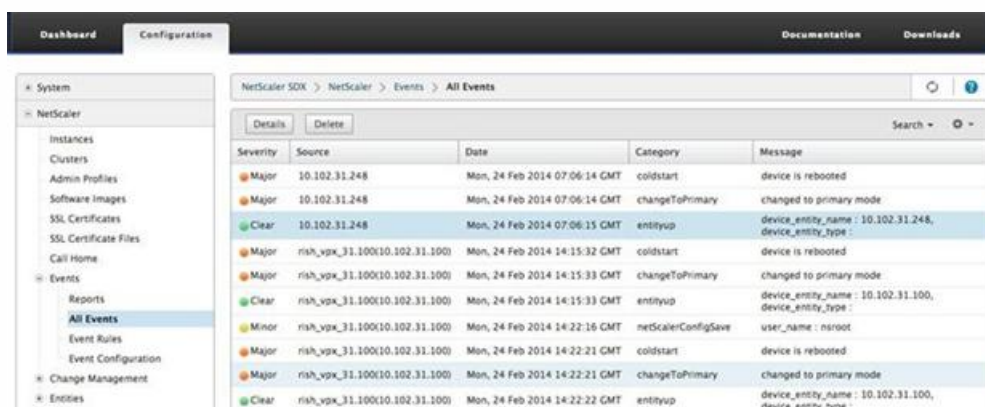
Apr 11, 2014

Use the Events feature to monitor and manage the events generated on the NetScaler instances. The Management Service identifies events in real time, thereby helping you address issues immediately and keep the NetScaler instances running effectively. You can also configure event rules to filter the events generated and get notified to take actions on the filtered list of events.

Viewing All Events

You can view all the events generated on the NetScaler instances provisioned on the NetScaler SDX appliance. You can view the details such as severity, category, date, source, and message for the each of the events.

To view the events, navigate to Configuration > NetScaler > Events > All Events



Severity	Source	Date	Category	Message
Major	10.102.31.248	Mon, 24 Feb 2014 07:06:14 GMT	coldstart	device is rebooted
Major	10.102.31.248	Mon, 24 Feb 2014 07:06:14 GMT	changeToPrimary	changed to primary mode
Clear	10.102.31.248	Mon, 24 Feb 2014 07:06:15 GMT	entityup	device_entity_name : 10.102.31.248, device_entity_type :
Major	rish_vpx_31.100(10.102.31.100)	Mon, 24 Feb 2014 14:15:32 GMT	coldstart	device is rebooted
Major	rish_vpx_31.100(10.102.31.100)	Mon, 24 Feb 2014 14:15:33 GMT	changeToPrimary	changed to primary mode
Clear	rish_vpx_31.100(10.102.31.100)	Mon, 24 Feb 2014 14:15:33 GMT	entityup	device_entity_name : 10.102.31.100, device_entity_type :
Minor	rish_vpx_31.100(10.102.31.100)	Mon, 24 Feb 2014 14:22:16 GMT	netScalerConfigSave	user_name : nsroot
Major	rish_vpx_31.100(10.102.31.100)	Mon, 24 Feb 2014 14:22:21 GMT	coldstart	device is rebooted
Major	rish_vpx_31.100(10.102.31.100)	Mon, 24 Feb 2014 14:22:21 GMT	changeToPrimary	changed to primary mode
Clear	rish_vpx_31.100(10.102.31.100)	Mon, 24 Feb 2014 14:22:22 GMT	entityup	device_entity_name : 10.102.31.100, device_entity_type :

You can view the event history and entity details by selecting the event and clicking the Details button. You can also search for a particular event or delete it from this page.

Note: After you delete the events, you will not be able to recover them.

Viewing Reports

The Reports page displays the events summary in a graphical format. Your view of the reports can be based on various time scales. By default the time scale is Day.

To display the reports, navigate to Configuration > NetScaler > Events > Reports. Following are the graphical reports supported on the Management Service

- **Events**

The Events report is a pie chart representation of the number of events, segmented and color coded on the basis of their severity.

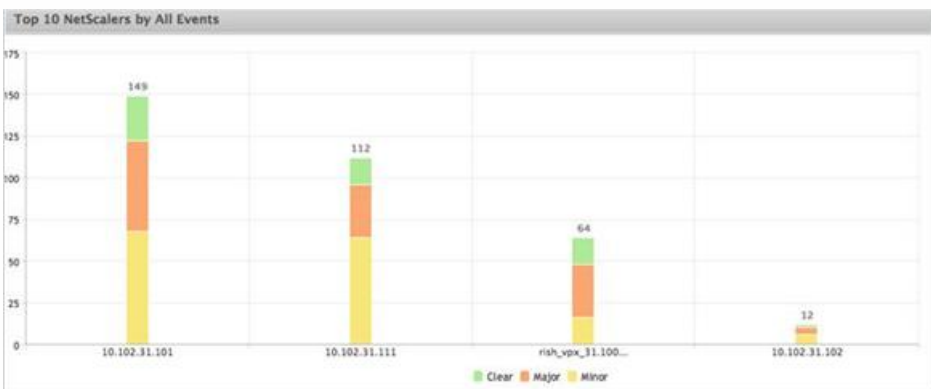


To view the details of the events of a particular severity, click that segment of the pie chart, you can view the following details:

- Source: System name, host name, or the IP address on which the event was generated.
- Date: Date and time when the alarm was generated.
- Category: Event category (for example, entityup).
- Message: Description of the event.

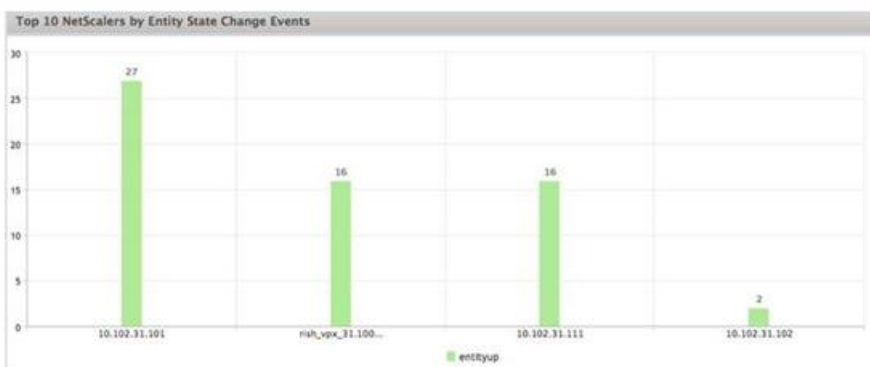
• **Top 10 NetScaler Instances by All Events**

This report is a bar chart that displays the top 10 NetScaler instances according to the number of events for the selected time scale.



• **Top 10 NetScaler Instances by Entity State Change Events**

This report is a bar chart that displays the top 10 NetScaler instances according to the number of entity state changes for the selected time scale. The entity state changes reflect entity up, entity down, or out of service events.



• **Top 10 NetScaler Instances by Threshold Violation Events**

This report is a bar chart that displays the top 10 NetScaler instances according to the number of threshold violation events for the selected time scale. The threshold violation events reflect the following events:

- cpuUtilization
- memoryUtilization
- diskUsageHigh
- temperatureHigh
- voltageLow
- voltageHigh
- fanSpeedLow
- temperatureCpuHigh
- interfaceThroughputLow
- interfaceBWUseHigh
- aggregateBWUseHigh



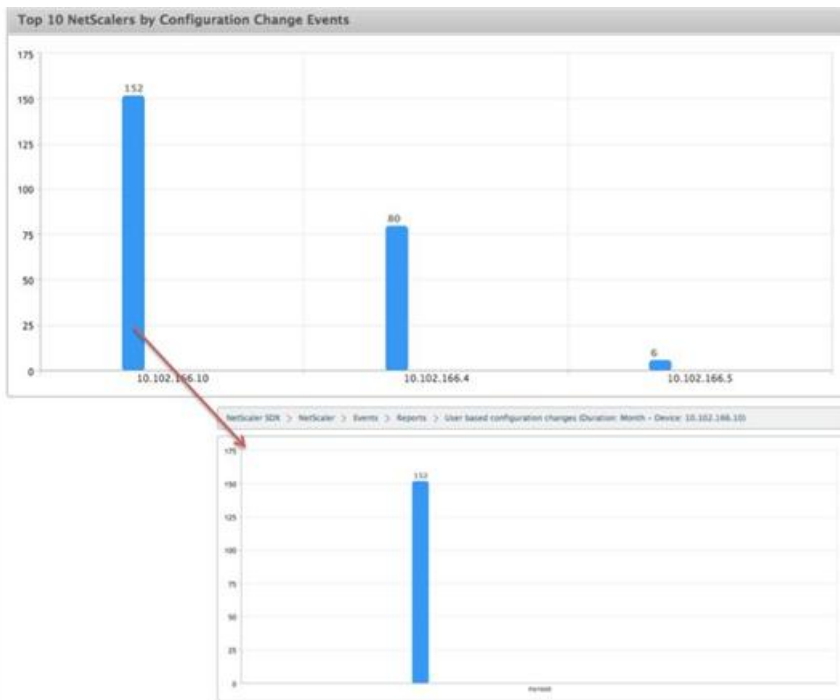
• **Top 10 NetScaler Instances by Hardware Failure Events**

This report is a bar chart that displays the top 10 NetScaler instances according to the number of hardware failure events for the selected time scale. The hardware failure events reflect the following events:

- hardDiskDriveErrors
- compactFlashErrors
- powerSupplyFailed
- "sslCardFailed"

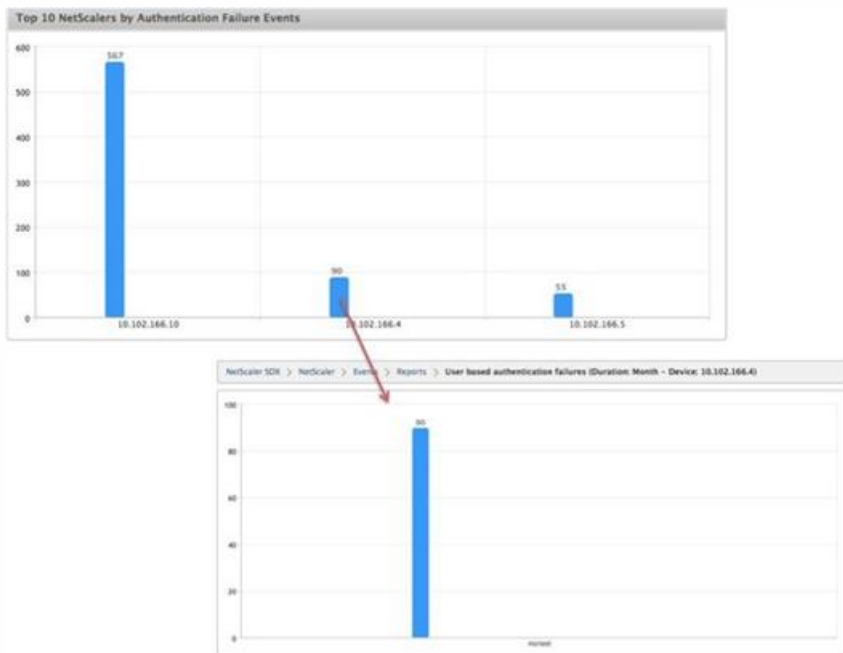
• **Top 10 NetScaler Instances by Configuration Change Events**

This report is a bar chart that reflects the top 10 NetScaler instances according to the number of configuration change events for the selected time scale. You can click on the chart to drill down and view the user based configuration changes for a particular instance. You can further view the authorization and execution status details by clicking on this chart.



- **Top 10 NetScaler Instances by Authentication Failure Events**

This report is a bar chart that displays the top 10 NetScaler instances according to the number of authentication failure events for the selected time scale. You can click on the chart to drill down and view the user based authentication failures for a particular instance.



Configuring Event Rules

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is executed. The conditions for which you can create filters are: severity, devices, failure objects, and category.

You can assign the following actions to the events:

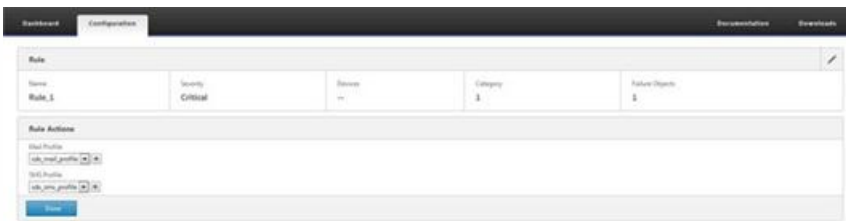
- Send e-mail Action: Sends an email for the events that match the filter criteria.
- Send SMS Action: Sends an Short Message Service(SMS) for the events that match the filter criteria.

To add event rules

1. Navigate to Configuration > NetScaler > Events > Event Rules, and click Add.
2. On the Rule page set the following parameters:
 - Name—Name of the event rule.
 - Enabled— Enable the event rule.
 - Severity— Severity of the events for which you want to add the event rule.
 - Devices— IP addresses of the NetScaler instances for which you want to define a event rule.
 - Category— Category or categories of the events generated by the NetScaler instances.
 - Failure Objects— Entity instances or counters for which an event has been generated.

Note: This list can contain counter names for all threshold-related events, entity names for all entity-related events, and certificate names for certificate-related events.

3. Click Save.
4. Under Rule Actions, you can assign the notification actions for the event.
 1. Mail Profile— Mail server and mail profile details. An email is triggered when the events meet the defined filter criteria.
 2. SMS Profile— SMS server and SMS profile details. An SMS is triggered when the events meet the defined filter criteria.



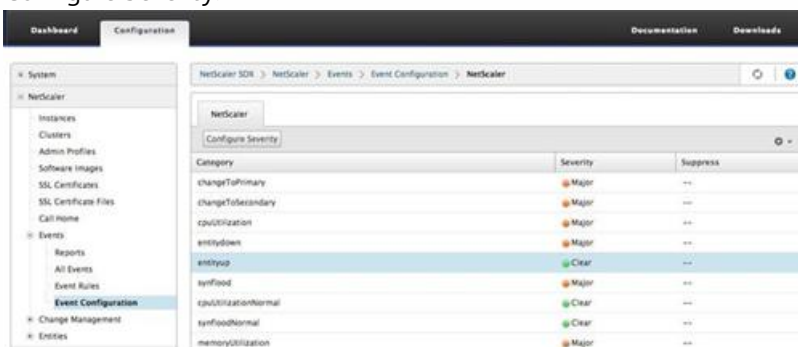
5. Click Done.

Configuring Events

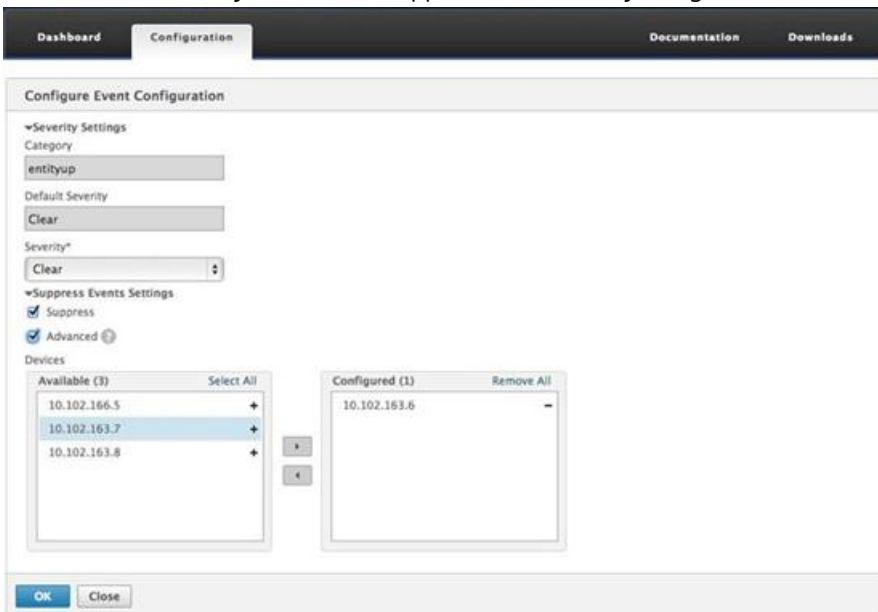
You can assign severity levels to events that are generated for the NetScaler instances on the NetScaler SDX appliance. You can define the following types of severity levels: Critical, Major, Minor, Warning, Clear, and Information. You can also suppress the events for a specific time.

To configure severity

1. Navigate to Configuration > NetScaler > Events > Event Configuration, select the event from the list, and then click Configure Severity.



2. On the Configure Events Configuration page, select the required severity level from the drop-down list.
3. Alternatively, you can suppress the events by selecting the Suppress check box. You can also specify the NetScaler instances for which you want to suppress this event by using the Advanced option.



4. Click OK.

Call Home Support for NetScaler Instances on NetScaler SDX

Apr 08, 2014

The Call Home feature monitors your NetScaler instances for common error conditions. You can now configure, enable or disable the Call Home feature on NetScaler instances from the Management Service user interface.

Note: The NetScaler instance has to be registered with the Citrix Technical Support server before Call Home can upload the system data to the server when predefined error conditions occur on the appliance. Enabling the Call Home feature on the NetScaler instance initiates the registration process.

Enabling and Disabling Call Home on a NetScaler Instance

You can enable the Call Home feature on NetScaler instance from the Management Service. When you enable the Call Home feature, the Call Home process registers the NetScaler instance with the Citrix Technical Support server. The registration takes some time to complete. During that time, the Management Service displays the progress of registration..

To enable the Call Home feature, navigate to Configuration > NetScaler > Call Home, select the NetScaler instance, and click the Enable button. In the confirmation page, click Yes.

To disable the Call Home feature, navigate to Configuration > NetScaler > Call Home, select the NetScaler instance, and click the Disable button. On the confirmation page, click Yes.

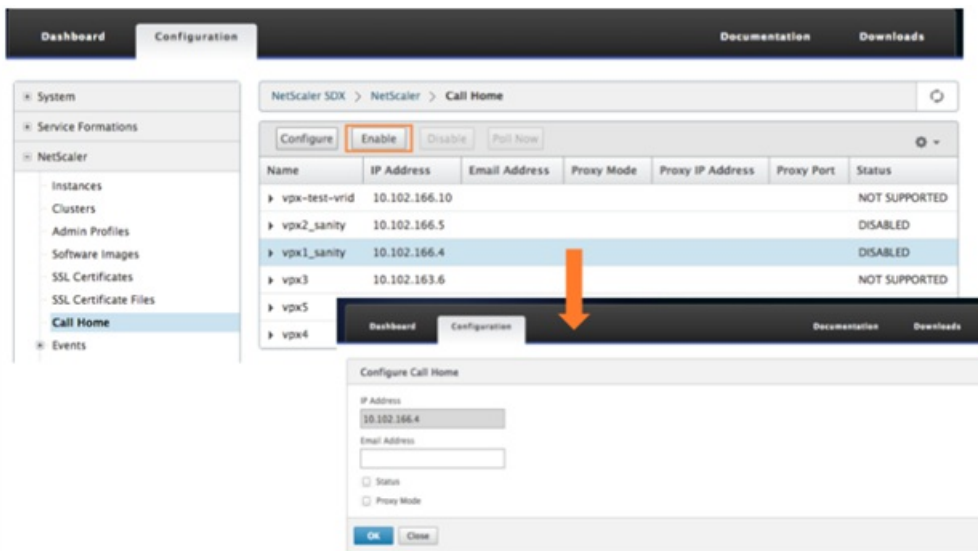
If you enable Call Home, you can configure the following options:

1. (Optional) Specify the administrator's email address. The Call Home process sends the email address to the Support server, where it is stored for future correspondence regarding Call Home.
2. (Optional) Enable Call Home proxy mode. Call Home can upload your NetScaler instance's data to the Citrix TaaS server through a proxy server. To use this feature, enable it on your NetScaler instance and specify the IP address and port number of an HTTP proxy server. All traffic from the proxy server to the TaaS servers (over the Internet) is over SSL and encrypted, so data security and privacy are not compromised.

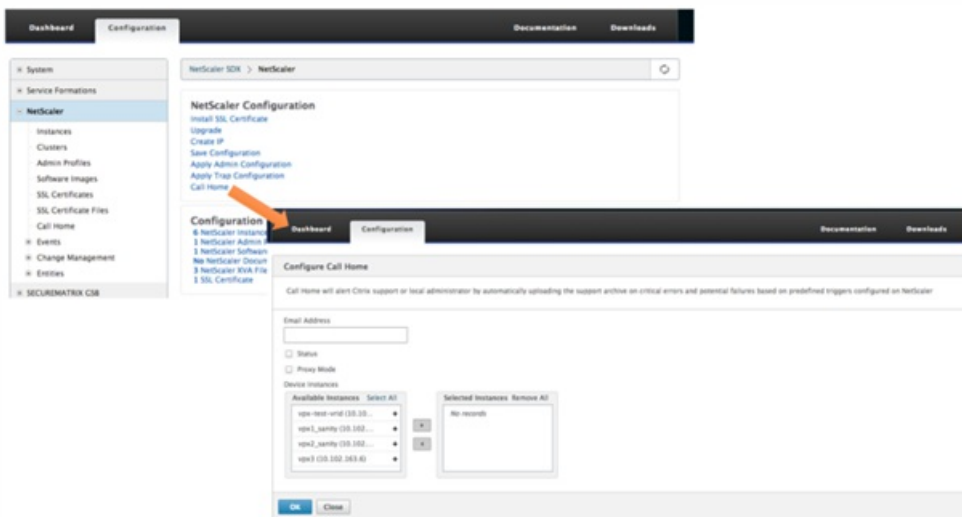
To configure Call home on the NetScaler instance from the Management Service

You can configure the Call Home feature on a single instance or on multiple instances at the same time.

To configure Call Home feature on a single NetScaler instance, navigate to Configuration > NetScaler > Call Home, select the NetScaler instance and click Configure button. In the Configure Call Home page, click OK.



To configure Call Home feature on a multiple NetScaler instances, navigate to Configuration > NetScaler, in the right pane, click Call Home, on the Configure Call Home page, select the NetScaler instances from the Available Instances section, specify other details, and click OK.



Polling the NetScaler Instances

To poll the Call Home feature from all NetScaler instances and view the current status, navigate to Configuration > NetScaler > Call Home, and click Poll Now button. On the confirmation page, click Yes.

System Health Monitoring

Apr 18, 2015

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 repository.

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

Jan 31, 2011

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.

If a task that you need to perform is not described below, see the list of tasks at the left.

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 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 instances. The 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.

Removing Management Service Files

Updated: 2013-10-07

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.

Command Line Interface support for Management Service

You can now use the command line interface to perform operations on the Management Service. The following operations are supported:

- Add, Set, Delete—To configure the resources.
- Do—To perform system level operations. For example, management service upgrade or shutdown, or reboot.
- Save—To add interfaces, which are used for NetScaler provisioning.

To access the CLI, start the secure shell (SSH) client from any workstation connected to the Management Service IP address. Log on by using the administrator credentials.

You can access detailed information about command usage and syntax from the man pages.

Note: CLI is not supported over console access.

Configuring Authentication and Authorization Settings

Oct 28, 2015

Note: External authentication support on a NetScaler SDX appliance is available only on NetScaler release 10.1.e.

Authentication with the NetScaler SDX Management Service can be local or external. With external authentication, the Management Service grants user access on the basis of the response from an external server. The Management Service supports the following external authentication protocols:

- Remote Authentication Dial In User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS)
- Lightweight Directory Access Protocol (LDAP)

The Management Service also supports authentication requests from SSH. The SSH authentication supports only keyboard-interactive authentication requests. The authorization of SSH users is limited to Superuser privileges only. Users with readonly privileges cannot log on through SSH.

To configure authentication, specify the authentication type, and configure an authentication server.

Authorization through the Management Service is local. The Management Service supports two levels of authorization. Users with superuser privileges are allowed to perform any action on the management service. Users with readonly privileges are allowed to perform only read operations. The authorization of SSH users is limited to superuser privileges only. Users with readonly privileges cannot log on through SSH.

Authorization for RADIUS and LDAP is supported by group extraction. You can set the group extraction attributes during the configuration of RADIUS or LDAP servers on the Management Service. The extracted group name is matched with the group names on the Management Service to determine the privileges given to the user. A user can belong to multiple groups. In that case, if any group to which the user belongs has superuser privileges, the user has superuser privileges. A Default Authentication group attribute can be set during configuration. This group is considered along with the extracted groups for authorization.

In the case of TACACS authorization, the TACACS server administrator must permit a special command, superuser for a user who is to have superuser privileges and deny this command for users with readonly privileges. When a user logs on to NetScaler SDX appliance, the Management Service checks if the user has permission to execute this command and if the user has permission, the user is assigned the superuser privileges else the user is assigned readonly privileges.

Note: External authentication support on a NetScaler SDX appliance is available only on NetScaler release 10.1.e. Groups are logical sets of users that need to access common information or perform similar kinds of tasks. You can organize users into groups defined by a set of common operations. By providing specific permissions to groups rather than individual users, you can save time when creating new users.

If you are using external authentication servers for authentication, groups in NetScaler SDX can be configured to match groups configured on authentication servers. When a user belonging to a group whose name matches a group on an authentication server, logs on and is authenticated, the user inherits the settings for the group in NetScaler SDX appliance.

Adding a User Group

To add a user group

1. On the **Configuration** tab, under **System**, expand **Administration**, and then click **Groups**.
2. In the details pane, click **Add**.

3. In the Create System Group dialogue box, set the following parameters:
 - Name—Name of the Group. Maximum length: 128
 - Permission—Actions that this group is authorized to perform. Possible values: superuser and readonly.
 - Users—Database users belonging to the Group. Select the users you want to add to the group.
4. Click **Create** and **Close**.

Configuring User Accounts

Updated: 2014-04-11

Note: External authentication support on a NetScaler SDX appliance is available only on NetScaler release 10.1.e. 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. On the **Configuration** tab, under **System**, expand **Administration**, 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. Maximum length: 128
 - 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.
 - Enable External Authentication—Enables external authentication for this user. Management Service attempts external authentication before database user authentication. If this parameter is disabled, user is not authenticated with the external authentication server.
 - Configure Session Timeout—Enables you to configure the time period for how long a user can remain active. Specify the following details:
 - Session Timeout—The time period for how long a user session can remain active.
 - Session Timeout Unit—The timeout unit, in minutes or hours.
 - Groups—Assign the groups to the user.*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, expand **Administration**, 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.

Setting the Authentication type

Updated: 2014-04-11

Note: External authentication support on a NetScaler SDX appliance is available only on NetScaler release 10.1.e. From the Management Service interface, you can specify local or external authentication. External authentication is disabled for local users by default. It can be enabled by checking the Enable External Authentication option when adding the local user or modifying the settings for the user.

Important: External authentication is supported only after you set up a RADIUS, LDAP, or TACACS authentication server.

To set the authentication type

1. On the Configuration tab, under System, click Authentication.
2. In the details pane, click Authentication Configuration.
3. Set the following parameters:
 - Server Type—Type of authentication server configured for user authentication. Possible values: LDAP, RADIUS, TACACS, and Local.
 - Server Name—Name of the authentication server configured in the Management Service. The menu lists all the servers configured for the selected authentication type.
 - Enable fallback local authentication—Alternatively, you can choose to authenticate a user with the local authentication when external authentication fails. This option is enabled by default.
4. Click OK.

Enable or Disable Basic Authentication

You can authenticate to the Management Service NITRO interface using basic authentication. By default, basic authentication is enabled in the SDX appliance. Perform the following to disable basic authentication using the Management Service interface.

To disable basic authentication:

1. On the **Configuration** tab, click **System**.
2. In the **System Settings** group, click **Change System Settings**.
3. In the **Configure System Settings** dialog box, clear the **Allow Basic Authentication** check box.
4. Click **OK**.

Configuring the External Authentication Server

Jan 31, 2011

Note: External authentication support on a NetScaler SDX appliance is available only on NetScaler release 10.1.e. The Management Service can authenticate users with local user accounts or by using an external authentication server. The appliance supports the following authentication types:

- Local—Authenticates to the Management Service by using a password, without reference to an external authentication server. User data is stored locally on the Management Service.
- RADIUS—Authenticates to an external RADIUS authentication server.
- LDAP—Authenticates to an external LDAP authentication server.
- TACACS—Authenticates to an external Terminal Access Controller Access-Control System (TACACS) authentication server.

To configure an external authentication, specify the authentication type, and configure an authentication server.

Adding a RADIUS Server

Note: External authentication support on a NetScaler SDX appliance is available only on NetScaler release 10.1.e. To configure RADIUS authentication, specify the authentication type as RADIUS, and configure the RADIUS authentication server.

Management Service supports RADIUS challenge response authentication according to the RADIUS specifications. RADIUS users can be configured with a one-time password on RADIUS server. When the user logs on to NetScaler SDX appliance the user is prompted to specify this one time password.

To add a RADIUS server

1. On the **Configuration** tab, under **System**, expand **Authentication**, and then click **Radius**.
2. In the details pane, click **Add**.

The screenshot shows the NetScaler SDX configuration interface. The left sidebar shows the navigation tree with 'System' expanded and 'Authentication' > 'Radius' selected. The main pane shows the 'Authentication > Servers' configuration page. A 'Create RADIUS server' dialog box is open, displaying the following fields and options:

- Name***: radchallenge
- IP Address***: [Empty]
- Port***: 1812
- Time-out(seconds)***: 3
- Details**:
 - Secret Key***: [Empty]
 - Confirm Secret Key***: [Empty]
 - NAS ID**: [Empty]
 - Enable NAS IP Address Extraction**
 - Group Vendor Identifier**: [Empty]
 - Group Prefix**: [Empty]
 - Group Attribute Type**: [Empty]
 - Group Separator**: [Empty]
 - IP Address Vendor Identifier**: [Empty]
 - Password Vendor Identifier**: [Empty]
 - IP Address Attribute Type**: [Empty]
 - Password Attribute Type**: [Empty]
 - Password Encoding***: pap
 - Default Authentication Group**: [Empty]
- Accounting**

Buttons: **Create**, **Close**

3. In the Create Radius Server dialogue box, type or select values for the parameters:
 - **Name***—Name of the server.
 - **IP Address***—Server IP address.
 - **Port***—Port on which the RADIUS server is running. Default value: 1812.

- Time-out*—Number of seconds the system will wait for a response from the RADIUS server. Default value: 3.
 - Secret Key*—Key shared between the client and the server. This information is required for communication between the system and the RADIUS server.
 - Enable NAS IP Address Extraction—If enabled, the system's IP address (Management Service IP) is sent to the server as the "nasip" in accordance with the RADIUS protocol.
 - NASID—If configured, this string is sent to the RADIUS server as the "nasid" in accordance with the RADIUS protocol.
 - Group Prefix—Prefix string that precedes group names within a RADIUS attribute for RADIUS group extraction.
 - Group Vendor ID—Vendor ID for using RADIUS group extraction.
 - Group Attribute Type—Attribute type for RADIUS group extraction.
 - Group Separator—Group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.
 - IP Address Vendor Identifier—Vendor ID of the attribute in the RADIUS which denotes the intranet IP. A value of 0 denotes that the attribute is not vendor encoded.
 - IP Address Attribute Type—Attribute type of the remote IP address attribute in a RADIUS response.
 - Password Vendor Identifier—Vendor ID of the password in the RADIUS response. Used to extract the user password.
 - Password Attribute Type—Attribute type of the password attribute in a RADIUS response.
 - Password Encoding—How passwords should be encoded in the RADIUS packets traveling from the system to the RADIUS server. Possible values: pap, chap, mschapv1, and mschapv2.
 - Default Authentication Group—Default group that is chosen when the authentication succeeds in addition to extracted groups.
 - Accounting—Enable Management Service to log audit information with RADIUS server.
4. Click Create, and then, click Close.

Adding an LDAP Authentication Server

Note: External authentication support on a NetScaler SDX appliance is available only on NetScaler release 10.1.e. To configure LDAP authentication, specify the authentication type as LDAP, and configure the LDAP authentication server.

To add an LDAP server

1. On the **Configuration** tab, under **System**, expand **Authentication**, and then click **LDAP**.
2. In the details pane, click **Add**.
3. In the Create LDAP Server dialogue box, type or select values for the parameters:
 - Name*—Name of the server.
 - IP Address*—Server IP address.
 - **Port***—Port on which the LDAP server is running. Default value: 389.
 - Time-out*—Number of seconds the system will wait for a response from the LDAP server.
 - Base DN—Base, or node where the LDAP search should start.
 - Type—Type of LDAP server. Possible values: Active Directory (AD) and Novell Directory Service (NDS).
 - Administrative Bind DN—Full distinguished name that is used to bind to the LDAP server.
 - Administrative Password—Password that is used to bind to the LDAP server.
 - Validate LDAP Certificate—Check this option to validate the certificate received from LDAP server.
 - LDAP Host Name—Hostname for the LDAP server. If the validateServerCert parameter is enabled, this parameter specifies the host name on the certificate from the LDAP server. A host-name mismatch causes a connection failure.
 - Server Logon Name Attribute—Name attribute used by the system to query the external LDAP server or an Active Directory.
 - Search Filter—String to be combined with the default LDAP user search string to form the value. For example, `vpnallowed=true` with `ldaplogi name samaccount` and the user-supplied username `bob` would yield an LDAP

search string of: (&(vpnallowed=true)(samaccount=bob).

- Group Attribute—Attribute name for group extraction from the LDAP server.
- Sub Attribute Name—Subattribute name for group extraction from the LDAP server.
- Security Type—Type of encryption for communication between the appliance and the authentication server. Possible values:

PLAINTEXT: No encryption required.

TLS: Communicate using TLS protocol.

SSL: Communicate using SSL Protocol

- Default Authentication Group—Default group that is chosen when the authentication succeeds in addition to extracted groups.
- Referrals—Enable following of LDAP referrals received from LDAP server.
- Maximum LDAP Referrals—Maximum number of LDAP referrals to follow.
- Enable Change Password—Allow user to modify the password if the password expires. You can change the password only when the Security Type configured is TLS or SSL.
- Enable Nested Group Extraction—Enable Nested Group extraction feature.
- Maximum Nesting Level—Number of levels at which group extraction is allowed.
- Group Name Identifier—Name that uniquely identifies a group in LDAP server.
- Group Search Attribute—LDAP group search attribute. Used to determine to which groups a group belongs.
- Group Search Subattribute—LDAP group search subattribute. Used to determine to which groups a group belongs.
- Group Search Filter—String to be combined with the default LDAP group search string to form the search value.

The screenshot shows the 'Create LDAP server' configuration window. The fields are filled with the following values:

- Name*: LDAP-10.102.39.102
- IP Address*: 10.102.39.102
- Port*: 389
- Type*: AD
- Time-out(seconds)*: 3
- Validate LDAP Certificate
- LDAP Host Name: (empty)
- Connection Settings:
 - Base DN(location of users): (empty)
 - Administrative Bind DN: (empty)
 - Administrative Password: (empty)
 - Confirm Administrative Password: (empty)
- Other Settings:
 - Server Logon Name Attribute: samAccountName
 - Search Filter: (empty)
 - Group Attribute: memberOf
 - Sub Attribute Name: CN
 - Security Type*: PLAINTEXT
 - Default Authentication Group: (empty)
 - Referrals
 - Maximum Referral Level: 0
 - Enable Change Password
- Nested Group Extraction:
 - Enable Nested Group Extraction
 - Maximum Nesting Level: 2
 - Group Name Identifier: (empty)
 - Group Search Attribute: (empty)
 - Group Search Subattribute: (empty)
 - Group Search Filter: (empty)

Buttons: Create, Close

4. Click Create, and then click Close.

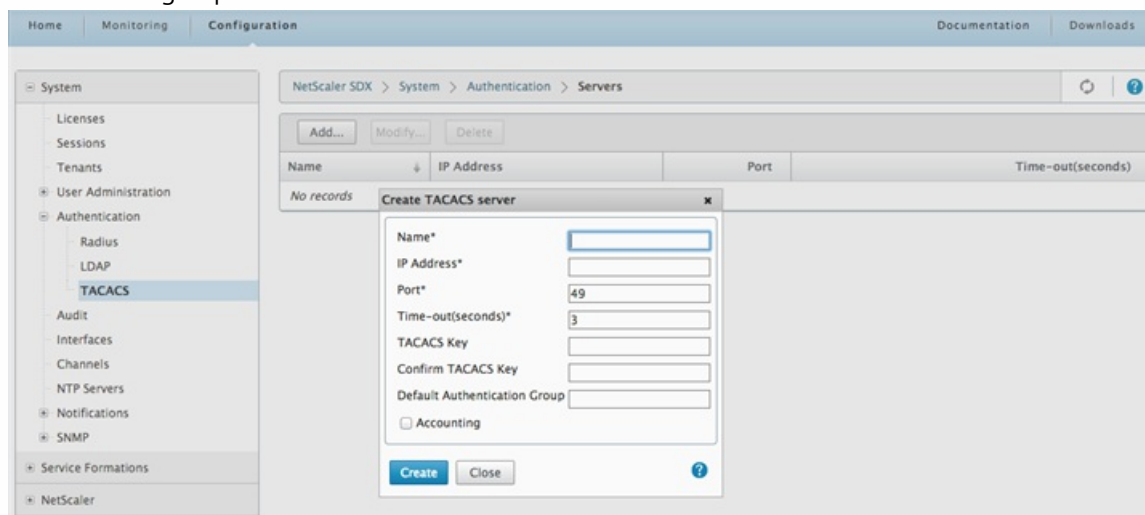
Adding a TACACS Server

Note: External authentication support on a NetScaler SDX appliance is available only on NetScaler release 10.1.e.

To configure TACACS authentication, specify the authentication type as TACACS, and configure the TACACS authentication server.

To add a TACACS server

1. On the **Configuration** tab, under **System**, expand **Authentication**, and then click **TACACS**.
2. In the details pane, click **Add**.
3. In the Create TACACS Server dialogue box, type or select values for the parameters:
 - Name—Name of the TACAS server
 - IP Address—IP address of the TACACS server
 - Port—Port on which the TACACS Server is running. Default value: 49
 - Time-out—Maximum number of seconds the system will wait for a response from the TACACS server
 - TACACS Key —Key shared between the client and the server. This information is required for the system to communicate with the TACACS server
 - Accounting—Enables Management Service to log audit information with TACACAS server.
 - Default Authentication Group—Default group that is chosen when the authentication succeeds in addition to extracted groups.



4. Click **Create**, and then click **Close**.

Configuring Link Aggregation from the Management Service

May 29, 2013

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

When a network interface is bound to a channel, the channel parameters have precedence over the network interface parameters. (That is, the network interface parameters are ignored.) A network interface can be bound only to one channel.

When a network interface is bound to a channel, it drops its VLAN configuration. The interface is removed from the VLAN that it originally belonged to and added to the default VLAN. However, you can bind the channel back to the old VLAN, or to a new one. For example, if you bind network interfaces 1/2 and 1/3 to a VLAN with ID 2 (VLAN 2), and then bind them to channel LA/1, the network interfaces are moved to the default VLAN, but you can bind the channel to VLAN 2.

Note:

- An interface must be part of only one channel.
- A minimum of two interfaces are required to configure a channel.
- The interfaces that form part of a channel are not listed in the Network Settings view when you add or modify a NetScaler instance. Instead of the interfaces, the channels are listed.

If you configure a channel by using three interfaces that are assigned to one instance, and a second instance uses some of these interfaces, the Management Service shuts down the second instance, modifies the network settings, and restarts the instance. For example, assume two instances, Instance1 and Instance2. When these instances are provisioned, interfaces 10/1, 10/2, and 10/3 are assigned to Instance1, and interfaces 10/1 and 10/2 are assigned to Instance2. If an LA channel is created with interfaces 10/1, 10/2, and 10/3, instance1 is not restarted. However, the Management Service shuts down Instance2, assigns interface 10/3 to Instance2, and then restarts Instance2.

If you remove an interface from an LA channel, the changes are stored in the database, and the interface appears in the Network Settings view when you add or modify an instance. Before you delete the interface, only the channel that the interface is a part of is listed.

Configuring a Channel from the Management Service

May 11, 2015

You can configure a channel manually, or you can use Link Aggregation Control Protocol (LACP). You cannot apply LACP to a manually configured channel, nor can you manually configure a channel created by LACP. You configure a channel from the Management Service and select the channel at the time of provisioning a NetScaler instance or later at the time of modifying a NetScaler instance.

To configure a channel from the Management Service

1. On the Configuration tab, navigate to System > Channels.
2. In the details pane, click Add.
3. In the Add Channel dialog box, set the following parameters:
 - Channel ID—ID for the LA channel to be created. Specify an LA channel in LA/x notation, where x can range from 1 to a number equal to one-half the number of interfaces. Cannot be changed after the LA channel is created.
 - Type—Type of channel. Possible values:
 - Static—configured only on the data interfaces.
 - Active-Active—configured only on the management interfaces 0/x.
 - Active-Passive—configured only on the management interfaces 0/x.
 - LACP—configured on data interfaces as well as the management interfaces 0/x.
 - Throughput (Applies only to a static channel and LACP)—Low threshold value for the throughput of the LA channel, in Mbps. In an HA configuration, failover is triggered if the LA channel has HA MON enabled and the throughput is below the specified threshold.
 - Bandwidth High (Applies only to a static channel and LACP)—High threshold value for the bandwidth usage of the LA channel, in Mbps. The appliance generates an SNMP trap message when the bandwidth usage of the LA channel is equal to or greater than the specified high threshold value.
 - Bandwidth Normal (Applies only to a static channel and LACP)—Normal threshold value for the bandwidth usage of the LA channel, in Mbps. When the bandwidth usage of the LA channel becomes equal to or less than the specified normal threshold after exceeding the high threshold, the NetScaler appliance generates an SNMP trap message to indicate that bandwidth usage has returned to normal.
4. On the Interfaces tab, add the interfaces that you want to include in this channel.
5. On the Settings tab, set the following parameters:
 - Channel State (Applies only to a static channel)—Enable or disable the LA channel.
 - LACP Time (Applies only to LACP)—Time after which a link is not aggregated if the link does not receive an LACPDU. The value must match on all the ports participating in link aggregation on the SDX appliance and the partner node.
 - HA Monitoring—In a High Availability (HA) configuration, monitor the channel for failure events. Failure of any LA channel that has HA MON enabled triggers HA failover.
 - Tag All—Add a four-byte 802.1q tag to every packet sent on this channel. The ON setting applies tags for all VLANs that are bound to this channel. OFF applies the tag for all VLANs other than the native VLAN.
 - Alias Name—Alias name for the LA channel. Used only to enhance readability. To perform any operations, you have to specify the LA channel ID.
6. Click Create, and then click Close.

Backing Up and Restoring the Configuration Data of the SDX Appliance

Feb 14, 2014

The backup policy runs at 00:30 A.M. every day. 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, or selected NetScaler instances.

To restore the configuration data on an SDX appliance, the Management Service selects the latest NetScaler .XVA image to provision the NetScaler instances. Citrix recommends that you store only the version of the NetScaler .XVA image that you require to reprovision the NetScaler instances. If you store multiple .XVA images, the Management Service might provision a NetScaler instance by using an image that is different from the one that you require. In this case, after restoring you must log on to the NetScaler instance and upgrade the software.

Important: You must manually back up other files, such as licenses and SSL certificates, outside the appliance before restoring the NetScaler instance because only the configuration files are restored.

To perform an immediate backup

1. Navigate to Configuration > Management Service > Backup Files.
2. In the Backup File pane, under **Action** drop-down list, 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. Navigate to Configuration > Management Service > Backup Files.
2. In the Backup File pane, select the backup file from the list, and then under **Action**, click Restore.
3. In the Restore dialog box, do 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.
 - Select the check box next to the instance(s) to restore the NetScaler instance(s).
4. Click OK.

Performing a Factory Reset

Dec 11, 2014

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.

Important: Make sure you connect a serial console cable to the appliance before performing a factory reset.

1. Under **Configuration** tab, in the navigation pane, expand Management Service > Backup Files, and then in the Action drop down menu select Factory Reset.
2. In the Factory Reset dialog box, select the type of reset option 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.
3. Click OK.
4. When the reset is complete, log on with the default credentials and run the configuration wizard.

Provisioning NetScaler Instances

Jan 31, 2011

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 [Creating Admin Profiles](#) above.

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.

Management LA

Select to associate the management channel to the instance.

VLAN Tag

Specify a VLAN ID for the management channel member interfaces.

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](#).

MAC Address Mode

Assign a MAC address. Select from 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. For information about setting a base MAC address, see Assigning a MAC Address to an Interface.

MAC Address

Specify a MAC address that overrides the generated MAC address. Used with the Custom mode setting.

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.

Restricting VLANs to Specific Virtual Interfaces

The NetScaler SDX appliance administrator can enforce specific 802.1Q VLANs on the virtual interfaces associated with NetScaler instances. This capability is especially helpful in restricting the usage of 802.1Q VLANs by the instance administrators. If two instances belonging to two different companies are hosted on an SDX appliance, you can restrict the two companies from using the same VLAN ID, so that one company does not see the other company's traffic. If an instance administrator, while provisioning or modifying a VPX instance, tries to assign an interface to an 802.1Q VLAN, a

validation is performed to verify that the VLAN ID specified is part of the allowed list.

By default, any VLAN ID can be used on an interface. To restrict the tagged VLANs on an interface, specify the VLAN IDs in the Network Settings at the time of provisioning a NetScaler instance, or later by modifying the instance. To specify a range, separate the IDs with a hyphen (for example 10-12). If you initially specify some VLAN IDs but later delete all of them from the allowed list, you can use any VLAN ID on that interface. In effect, you have restored the default setting.

After creating a list of allowed VLANs, the SDX administrator does not have to log on to an instance to create the VLANs. The administrator can add and delete VLANs for specific instances from the Management Service.

Important: If L2 mode is enabled, the administrator must take care that the VLAN IDs on different NetScaler instances do not overlap.

To specify the permitted VLAN IDs

1. In the Provision NetScaler Wizard or the Modify NetScaler Wizard, on the Network Settings page, in the Allowed VLANs text box, specify the VLAN ID(s) allowed on this interface. Use a hyphen to specify a range. For example, 2-4094.
2. Follow the instructions in the wizard.
3. Click Finish, and then click Close.

To configure VLANs for an instance from the Management Service

1. On the Configuration tab, navigate to NetScaler > Instances.
2. Select an instance, and then click VLAN.
3. In the details pane, click Add.
4. In the Create NetScaler VLAN dialog box, specify the following parameters:
 - VLAN ID—An integer that uniquely identifies the VLAN to which a particular frame belongs. The NetScaler supports a maximum of 4094 VLANs. ID 1 is reserved for the default VLAN.
 - IPV6 Dynamic Routing—Enable all IPv6 dynamic routing protocols on this VLAN. Note: For the ENABLED setting to work, you must log on to the instance and configure IPv6 dynamic routing protocols from the VTYSH command line.
5. Select the interfaces that should be part of the VLAN.
6. Click Create, and then click Close.

Setting up a Cluster of NetScaler Instances

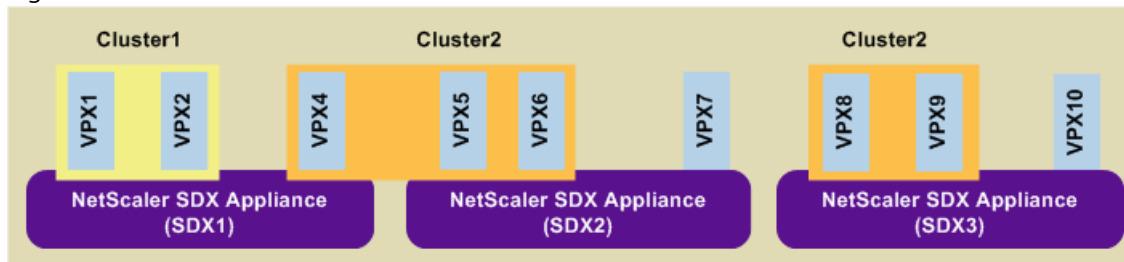
Sep 29, 2014

After provisioning NetScaler instances on one or more NetScaler SDX appliances, you can create a cluster of NetScaler instances. The nodes of the cluster can be NetScaler instances on the same SDX appliance or on other SDX appliances that are available on the same subnet.

Note:

- To set up a cluster, you must understand NetScaler clustering. For more information, see [Clustering](#).
- For clusters that have NetScaler instances across SDX appliances, Citrix recommends that you use NetScaler instances from three SDX appliances. This ensures that the cluster criteria of a minimum of $(n/2 + 1)$ nodes is always satisfied.

Figure 1. Cluster of SDX NetScaler instances



The above figure shows three SDX appliances, SDX1, SDX2, and SDX3, on the same subnet. The NetScaler instances on these appliances are used to form two clusters: Cluster1 and Cluster2.

- Cluster1 includes two instances on SDX1.
- Cluster2 includes one instance on SDX1, two instances on SDX2, and another two instances on SDX3.

Points to remember

- All nodes of a cluster must be of the same type. You cannot form a cluster of hardware and virtual appliances, nor a cluster of VPX NetScaler instances and SDX NetScaler instances.
- The NetScaler instances must be of the same version, which must be version 10.1 or later.
- The NetScaler instances must all have the same feature license.
- No configurations can be updated on individual NetScaler instances after they are added to the cluster. All changes must be performed through the cluster IP address.
- The NetScaler instances must all have the same resources (memory, CPU, interfaces, and so on).
- Cluster link aggregation is not supported on a cluster of SDX appliances.

To set up a NetScaler cluster on an SDX appliance

1. Log on to the SDX appliance.
2. On the Configuration tab, navigate to NetScaler, and then click Clusters.
3. Create the cluster:
 1. Click Create Cluster.
 2. In the Create Cluster dialog box, set the parameters required for the cluster. For a description of a parameter, hover the mouse cursor over the corresponding field.
 3. Click Next to view the configuration summary.
 4. Click Finish to create the cluster.

Note: When a NetScaler instance that is provisioned on the NetScaler SDX appliance has L2 VLAN configured, and if that node is added to the cluster, then the add vlan command is saved with the sdxvlan parameter set to Yes. This parameter is an internal argument and is used to avoid loss of connectivity during SDX cluster formation.

4. Add nodes to the cluster:

1. Click Add Node.
2. In the Add Node dialog box, configure the parameters required for adding a cluster node. For a description of a parameter, hover the mouse cursor over the corresponding field.
3. Click Next to view the configuration summary.
4. Click Finish to add the node to the cluster.
5. Repeat steps a through d to add another node to the cluster.

After creating the cluster, you must configure it by accessing it through the cluster IP address.

Note: To get an updated list of NetScaler clusters, each of which has at least one NetScaler instance of the SDX appliance, use the Rediscover option.

To add a NetScaler instance that exists on one SDX appliance to a cluster configured on another SDX appliance

1. Log on to the SDX appliance from which you want to add the NetScaler instance.
2. On the Configuration tab, navigate to NetScaler, and then click Clusters.
3. Click Add Node.
4. In the Add Node dialog box, configure the parameters required for adding a cluster node. For a description of a parameter, hover the mouse cursor over the corresponding field.

Note: Make sure the values of the Cluster IP address and Cluster IP Password parameters are for the cluster to which you want to add the node.

5. Click Next to view the configuration summary.
6. Click Finish to add the node to the cluster.

Configuring and Managing NetScaler Instances

Jan 31, 2011

After you have provisioned NetScaler instances on your appliance, you are ready to configure and manage the instances. Begin by creating a subnet IP (SNIP) or mapped IP (MIP) address and then saving the configuration. You can then perform basic management tasks on the instances. Check to see if you have to apply the administration configuration.

If a task that you need to perform is not described below, see the list of tasks at the left.

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.

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.

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.

Installing and Managing SSL Certificates

Jan 31, 2011

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.

Allowing L2 Mode on a NetScaler Instance

Jul 08, 2013

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

Dec 05, 2012

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.

Change Management for NetScaler VPX Instances

Jul 10, 2013

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. You can create an audit template by copying the commands from an existing configuration file. You can later use this template to find any changes in the configuration of an instance and take corrective action if required.

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 from the Action list, 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).
 - Template Diff—Displays the difference between the saved or running configuration and the template. You can save this difference as a batch file. To apply the configuration from the template to the instance, apply this batch file to the instance.
 - 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, from the Action list, 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.

To configure an audit template for a NetScaler instance

1. Open an existing configuration file and copy its list of commands.
2. On the Configuration tab, navigate to NetScaler > Change Management > Audit Templates.
3. In the details pane, click Add.
4. In the Add Template dialog box, add a name and description for the template.
5. In the Command text box, paste the list of commands that you copied from the configuration file
6. Click Create, and then click Close.

Monitoring NetScaler Instances

Apr 18, 2015

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 NetScaler VPX instances

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

Apr 18, 2015

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 the 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.

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.

3.

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 Appliances

Jun 03, 2014

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

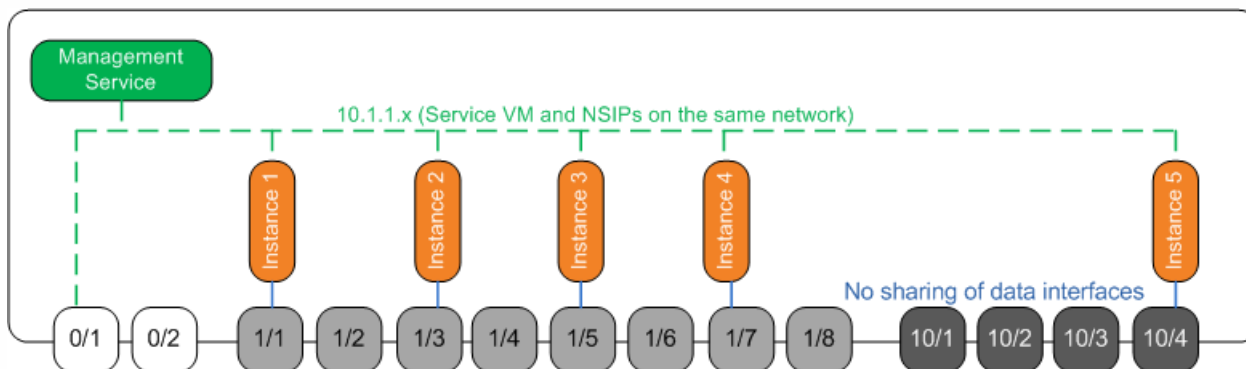
Apr 12, 2013

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

Parameter Name	Values for Instance 1
XVA File	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature License	Platinum
Admin Profile	ns_nsroot_profile
User Name	vp8
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

Apr 12, 2013

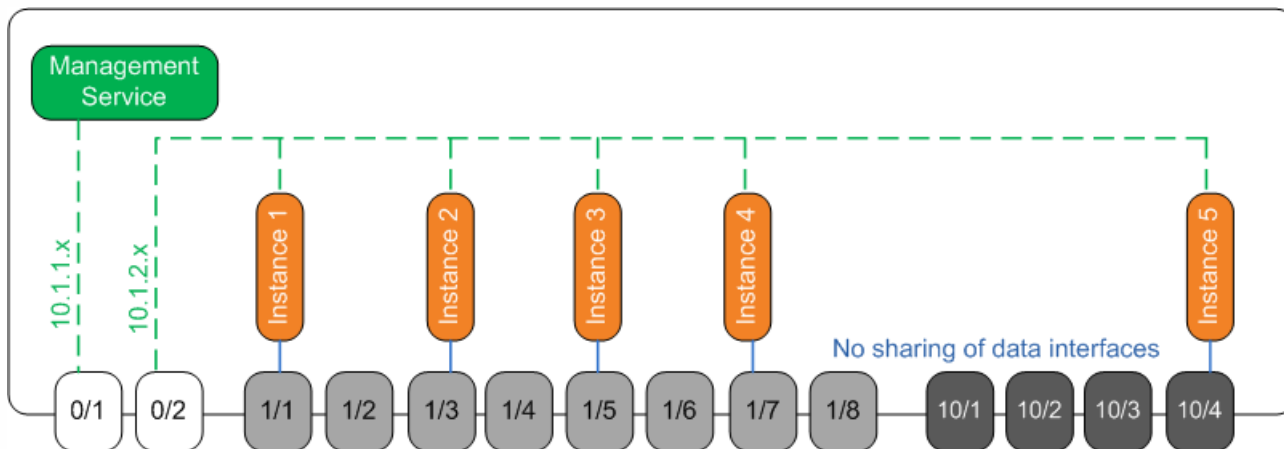
In certain cases, the appliance administrator might allow other administrators to perform administration tasks on individual instances. This can be safely done by giving an individual instance administrator login rights to just that instance. But, for security reasons, the appliance administrator might 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

Parameter Name	Values for Instance 1
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

Jan 31, 2011

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.

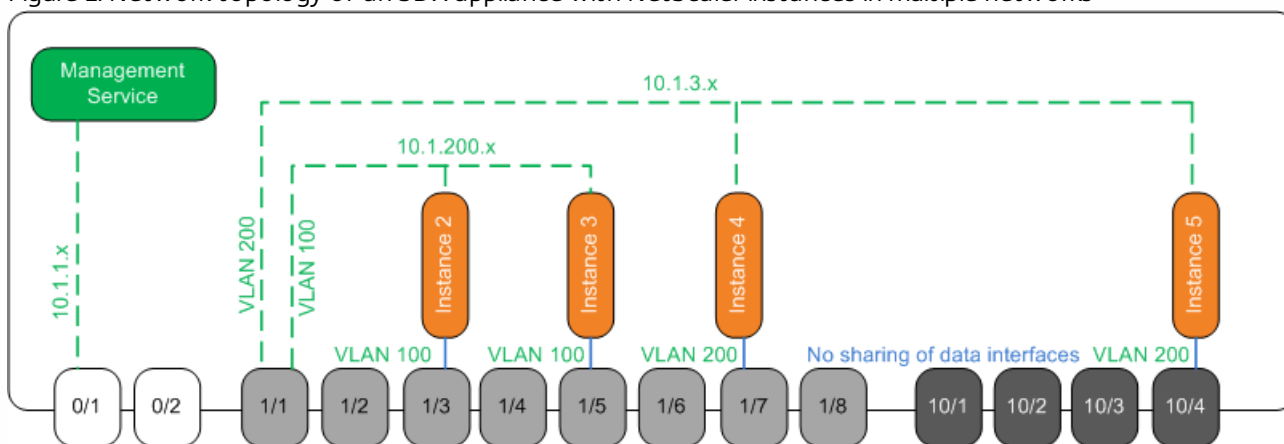
Consolidation with Dedicated Interfaces for Each Instance

Apr 12, 2013

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	vp5	vp3
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

Parameter Name Admin Profile	Values for Instance 5 ns_nsroot_profile	Values for Instance 3 ns_nsroot_profile
User Name	vp5	vp3
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

Apr 12, 2013

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.

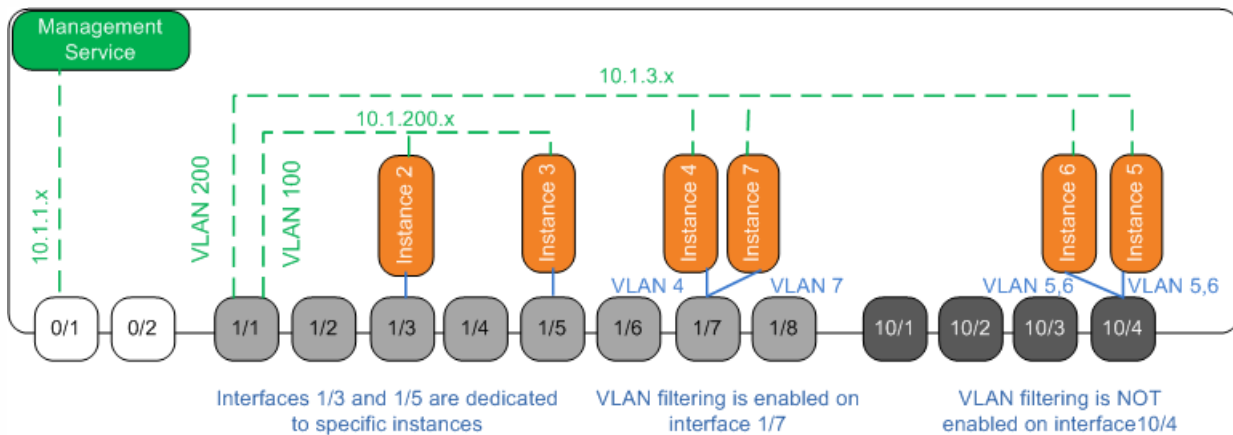
Note: VLAN filtering is not a global setting on the appliance. You enable or disable VLAN filtering on an interface, and the setting applies to all instances associated with that interface. If VLAN filtering is disabled, you can configure up to 4096 VLANs. If VLAN filtering is enabled, you can configure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

Parameter Name	Values for Instance 7	Values for Instance 4
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.

Converting a NetScaler MPX Appliance to a NetScaler SDX Appliance

Jan 28, 2011

You can convert a NetScaler MPX appliance to a NetScaler SDX appliance to deploy multiple virtualized NetScaler instances on a single, purpose-built physical appliance with full multiservice and multitenant support.

You can convert the NetScaler MPX 11515/11520/11530/11540/11542 appliances to NetScaler SDX 11515/11520/11530/11540/11542 appliances by upgrading the software through a new Solid State Drive (SSD) and a new Hard Disk Drive (HDD).

The Citrix NetScaler models SDX 11515/11520/11530/11540/11542 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory.

The SDX 11515/11520/11530/11540/11542 appliances have the following ports:

- RS232 serial console port.
- 10/100Base-T copper Ethernet Port (RJ45), also called the LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
Note: The LEDs on the LOM port are not operational, by design.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45), numbered 0/1 and 0/2 from left to right. These ports are used to connect directly to the appliance for system administration functions. Eight 10G SFP+ ports and four copper or fiber 1G SFP ports.

You can convert the NetScaler MPX 8200/8400/8600/8800 appliances to NetScaler SDX 8400/8600 appliances by upgrading the software through a new Solid State Drive (SSD).

The Citrix NetScaler models SDX 8400 and SDX 8600 are 1U appliances. Each model has one quad-core processor (8 cores with hyper-threading) and 32 gigabytes (GB) of memory. The SDX 8400/8600 appliances are available in two port configurations:

- Six 10/100/1000Base-T copper Ethernet ports and six 1G SFP ports (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP)
- Six 10/100/1000Base-T copper Ethernet ports and two 10G SFP+ ports (6x10/100/1000Base-T copper Ethernet ports + 2x10G SFP+)

Converting a NetScaler MPX 11515/11520/11530/11540/11542 Appliance to a NetScaler SDX 11515/11520/11530/11540/11542 Appliance

Jan 07, 2014

You can convert a NetScaler MPX appliance to a NetScaler SDX appliance by upgrading the software through a new Solid State Drive (SSD) and a new Hard Disk Drive (HDD). Citrix supplies a field conversion kit to migrate a NetScaler MPX appliance to a NetScaler SDX appliance.

Note: Citrix recommends that you configure the Lights Out Management (LOM) Port of the NetScaler appliance before starting the conversion process. For more information on the LOM port of the NetScaler appliance, see [Lights Out Management Port of the NetScaler Appliance](#).

To convert a NetScaler MPX appliance to a NetScaler SDX appliance, you must access the appliance through a console cable attached to a computer or terminal. Before connecting the console cable, configure the computer or terminal to support the following configuration:

- VT100 terminal emulation
- 9600 baud
- 8 data bits
- 1 stop bit
- Parity and flow control set to NONE

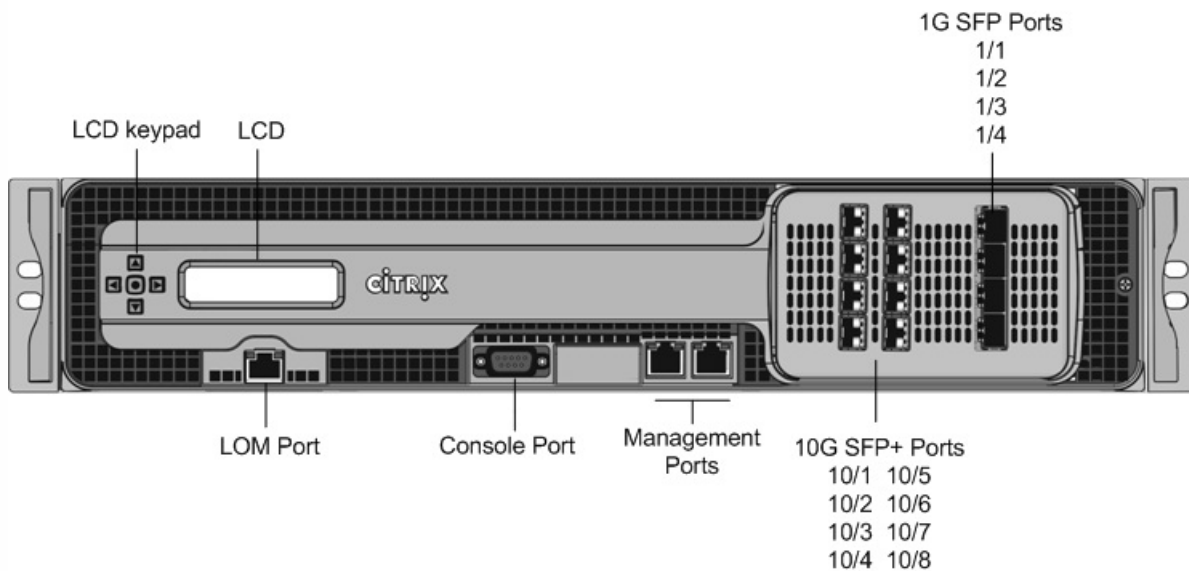
Connect one end of the console cable to the RS232 serial port on the appliance, and the other end to the computer or terminal.

Note: To use a cable with an RJ-45 converter, insert the optional converter into the console port and attach the cable to it. With the cable attached, verify that the MPX appliance's components are functioning correctly. You are then ready to begin the conversion. The conversion process modifies the Basic Input-Output System (BIOS), installs XenServer hypervisor and a Service Virtual Machine image, and copies the NetScaler VPX image to the Hard Disk Drive.

After the conversion process, you make a few modifications to the appliance's configuration and apply a new license. You can then provision the VPX instances through the Management Service on what is now a NetScaler SDX appliance.

The following figure shows the front panel of the MPX 11515/11520/11530/11540/11542 appliance.

Figure 1. Citrix NetScaler MPX 11515/11520/11530/11540/11542, front panel



To verify proper operation of the MPX appliance's components

1. Access the console port and enter the administrator credentials.
2. Run the following command from the command line interface of the appliance to display the serial number: **show hardware**

The serial number might be helpful in the event that you want to contact Citrix Technical Support.

Example

```
> show hardware
Platform: NSMPX-11500 12*CPU+8*IX+4*E1K+2*E1K+2*CVM N3 1400210
Manufactured on: 8/12/2014
CPU: 2400MHZ
Host Id: 872841350
Serial no: 2NSHJ2DR9E
Encoded serial no: 2NSHJ2DR9E
```

Done

3. Run the following command to display the status of the active 1G and 10G interfaces: **show interface**
4. In the show interface command's output, verify that all of the interfaces are enabled and the status of every interface is shown as UP/UP.
Note: If you do not have an SFP+ transceiver for every port, verify the interfaces in stages. After checking the first set of interfaces, unplug the SFP+ transceivers and plug them in to the next set of ports. The SFP+ transceivers are not hot-swappable. Therefore, restart the MPX appliance after you connect the transceivers.
5. Run the following commands for each of the interfaces that are not in the UP/UP state:

- **enable interface 1/x**
- **enable interface 10/x**

where x is the new interface number.

6. Run the following command to verify that the status of the power supplies is normal: **stat system -detail**

Example

```
> stat system -detail
NetScaler Executive View
```

System Information:

Up since Wed Aug 13 12:09:54 2014
Memory usage (MB) 924
InUse Memory (%) 5.64
Number of CPUs 5

System Health Statistics (Standard):

CPU 0 Core Voltage (Volts) 1.10
CPU 1 Core Voltage (Volts) 1.10
Main 3.3 V Supply Voltage 3.26
Standby 3.3 V Supply Voltage 3.22
+5.0 V Supply Voltage 5.09
+12.0 V Supply Voltage 12.14
Battery Voltage (Volts) 3.17
Intel CPU Vtt Power(Volts) 0.00
5V Standby Voltage(Volts) 4.97
Voltage Sensor2(Volts) 0.00
CPU Fan 0 Speed (RPM) 5929
CPU Fan 1 Speed (RPM) 5929
System Fan Speed (RPM) 5929
System Fan 1 Speed (RPM) 5929
System Fan 2 Speed (RPM) 5929
CPU 0 Temperature (Celsius) 49
CPU 1 Temperature (Celsius) 51
Internal Temperature (Celsius) 33
Power supply 1 status NORMAL
Power supply 2 status NORMAL

System Disk Statistics:

/flash Size (MB) 63473
/flash Used (MB) 149
/flash Available (MB) 58246
/flash Used (%) 0
/var Size (MB) 745163
/var Used (MB) 249
/var Available (MB) 685300
/var Used (%) 0

System Health Statistics(Auxiliary):

Voltage 0 (Volts) 0.00
Voltage 1 (Volts) 0.00
Voltage 2 (Volts) 0.00
Voltage 3 (Volts) 0.00
Voltage 4 (Volts) 1.50
Voltage 5 (Volts) 0.00
Voltage 6 (Volts) 0.00

```

Voltage 7 (Volts)          0.00
Fan 0 Speed (RPM)         5929
Fan 1 Speed (RPM)         0
Fan 2 Speed (RPM)         0
Fan 3 Speed (RPM)         0
Temperature 0 (Celsius)   40
Temperature 1 (Celsius)   35
Temperature 2 (Celsius)   0
Temperature 3 (Celsius)   0
Done

```

- Run the following command to generate a tar of system configuration data and statistics: **show techsupport**
Example

```

> show techsupport
showtechsupport data collector tool - $Revision: #1 $! NetScaler version 9.2
The NS IP of this box is 10.10.10.10
Current HA state: Primary (or this is not part of HA
pair!)
All the data will be collected under

```

```

/var/tmp/support/collector_10.10.10.10_P_13May2011_12_01

```

```

Copying selected configuration files from nsconfig ....

```

Note: The output of the command is available in the /var/tmp/support/collector_<IP_address>_P_<date>.tar.gz file. Copy this file to another computer for future reference. The output of the command might be helpful in the event that you want to contact Citrix Technical Support.

- At the NetScaler command line interface, switch to the shell prompt. Type: **shell**
- Run the following command to verify that 2 Cavium cards are available: **root@ns# dmesg | grep cavium**
Example

```

root@ns# dmesg | grep cavium
Cavium cavium_probe : found card 0x177d,device=0x11
cavium0 mem 0xdd00000-0xddffff irq 24 at device 0.0 on pci20
Cavium cavium_probe : found card 0x177d,device=0x11
cavium1 mem 0xd6f0000-0xd6ffff irq 32 at device 0.0 on pci5
Run the following command to verify that 596 MB of RAM is reserved for shared memory: root@ns# dmesg | grep
memory

```

Example

```

root@ns# dmesg | grep memory
real memory = 52613349376 (50176 MB)
avail memory = 49645355008 (47345 MB)
NS-KERN map_shared_mem_ioctI (cpu 7, NSPPE-03): Reserving 596 MB for shared memory type 0

```

- Run the following command to verify that the appliance has 12 CPU cores: **root@ns# dmesg | grep cpu**
Example

```

root@ns# dmesg | grep cpu
cpu0 (BSP): APIC ID: 0

```

```

cpu1 (AP): APIC ID: 2
cpu2 (AP): APIC ID: 4
cpu3 (AP): APIC ID: 16
cpu4 (AP): APIC ID: 18
cpu5 (AP): APIC ID: 20
cpu6 (AP): APIC ID: 32
cpu7 (AP): APIC ID: 34
cpu8 (AP): APIC ID: 36
cpu9 (AP): APIC ID: 48
cpu10 (AP): APIC ID: 50
cpu11 (AP): APIC ID: 52
cpu0: <ACPI CPU> on acpi0
acpi_throttle0: <ACPI CPU Throttling> on cpu0
cpu1: <ACPI CPU> on acpi0
acpi_throttle1: <ACPI CPU Throttling> on cpu1
cpu2: <ACPI CPU> on acpi0
cpu3: <ACPI CPU> on acpi0
cpu4: <ACPI CPU> on acpi0
cpu5: <ACPI CPU> on acpi0
cpu6: <ACPI CPU> on acpi0
cpu7: <ACPI CPU> on acpi0
cpu8: <ACPI CPU> on acpi0
cpu9: <ACPI CPU> on acpi0
cpu10: <ACPI CPU> on acpi0
cpu11: <ACPI CPU> on acpi0
NS-KERN map_shared_mem_ioctl (cpu 7, NSPPE-03): Reserving 596 MB for shared memory type 0

```

11. Run the following command to verify that the /var drive is mounted as /dev/ad8s1e: **root@ns# df -h**

Example

```

root@ns# df -h
Filesystem      Size  Used Avail Capacity  Mounted on
/dev/md0c       276M  246M   24M   91%    /
devfs           1.0K  1.0K   0B   100%  /dev
procfs         4.0K  4.0K   0B   100%  /proc
/dev/ad4s1a     62G   149M   57G    0%    /flash
/dev/ad8s1e    728G   299M  669G    0%    /var
root@ns#

```

12. Run the following command to execute the ns_hw_err.bash script, which checks for latent hardware errors: **root@ns#**

/netscaler/ns_hw_err.bash

Example

```

root@ns# /netscaler/ns_hw_err.bash
NetScaler NS10.1: Build 127.11.nc, Date: Aug 11 2014, 18:24:36
platform: serial 2NSHJ2DR9E
platform: sysid 1400210 - NSMPX-11500 12*CPU+8*IX+4*E1K+2*E1K+2*CVM N3
HDD MODEL: Device Model: ST1000NM0033-9ZM173

```

```

Generating the list of newslog files to be processed...
Generating the events from newslog files...
Checking for HDD errors...
/var/nslog/dmesg.prev:swap.NO
*****
HDD ERROR: FOUND      1 HDD errors: swap.NO
*****
Checking for HDD SMART errors...
Checking for Flash errors...
Checking for SSL errors...
Checking for BIOS errors...
Checking for SMB errors...
Checking for MotherBoard errors...
Checking for CMOS errors...
    License year: 2014: OK
License server failed at startup. Check /var/log/license.log
Vendor daemon failed at startup. Check /var/log/license.log
Checking for SFP/NIC errors...
Checking for Firmware errors...
Checking for License errors...
Checking for Undetected CPUs...
Checking for DIMM flaps...
Checking the Power Supply Errors...
root@ns#

```

13. **Important:** Physically disconnect all ports except the LOM port, including the management port, from the network.
14. At the shell prompt, switch to the NetScaler command line. Type: **exit**
15. Run the following command to shut down the appliance: **shutdown -p now**

Example

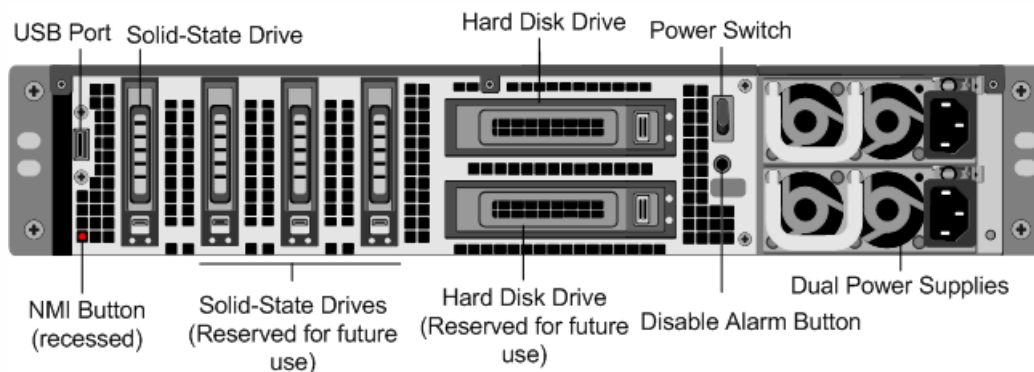
```

> shutdown -p now
Are you sure you want to completely stop NetScaler (Y/N)? [N]:y

```

To upgrade the appliance

1. Locate the solid-state drive on the back panel of the appliance, as shown in the following figure:



2. Verify that the replacement solid-state drive (SSD) is the one required for your NetScaler model. The Citrix label is on the top of the solid-state drive, which is pre-populated with a new version of BIOS and a recent build of the required Service VM software.
3. Remove the SSD drive by pushing the safety latch of the drive cover down while pulling the drive handle.
4. On the new SSD drive, open the drive handle completely, and then insert the new drive into the slot.
5. Close the handle flush with the rear side of the appliance so that the drive locks securely into the slot.
Important: The orientation of the solid-state drive is important. When you insert the drive, make sure that the Citrix product label is at the top.
6. Locate the hard disk drive (HDD) on the back panel of the appliance.
7. Remove the HDD by pushing the safety latch of the drive cover to the right and pulling the drive handle.
8. On the new disk drive, open the drive handle completely to the left, and then insert the new drive into the slot.
9. Close the handle flush with the rear side of the appliance so that the hard drive locks securely into the slot.
10. Store the old SSD/HDD pair for future handling.

Important: The orientation of the hard disk drive is important. When you insert the drive, make sure that the Citrix product label is at the top.

11. Start the NetScaler appliance. For instructions, see [Switching on the Appliance](#).

The conversion process takes approximately 30 minutes to complete. The conversion process updates the BIOS, installs the XenServer hypervisor and the Management Service Operating system, and copies the NetScaler VPX image to the hard disk drive for instance provisioning. When the conversion begins, the LCD screen on the front bezel indicates NSMPX-11500 10G, as shown in the following figure.



When the conversion is successful, the LCD indicates Citrix NSSDX - 11515, as shown in the following figure.



Note: The serial number of the appliance remains the same.

12. Keep the console cable attached during the conversion process. Allow the process to complete, at which point the `netScaler-sdx login:` prompt appears.

If the boot SSD is not inserted completely into the designated slot, the NetScaler SDX appliance attempts to start from the hard disk drive, and the bootup process results in a prompt different from the one mentioned above. If the `netScaler-sdx login:` prompt does not appear, carefully re-seat the SSD, close the locking handle, and restart the appliance.

To reconfigure the converted appliance

After the conversion process, the appliance no longer has its previous working configuration. Therefore, you can access the appliance through a Web browser only by using the default IP address: 192.168.100.1/16. Configure a computer on network 192.168.0.0 and connect it directly to the appliance's management port (0/1) with a cross-over Ethernet cable, or access the NetScaler SDX appliance through a network hub by using a straight through Ethernet cable. Use the default credentials to log on (**Username:** nsroot and **Password:** nsroot), and then do the following:

1. Select the Configuration tab.
2. Verify that the System Resource section displays 24 CPU cores, 16 SSL cores, 48 GB of total memory for the NetScaler SDX appliance.

The screenshot shows the NetScaler SDX Configuration page. The top navigation bar includes 'Home', 'Monitoring', and 'Configuration'. The 'Configuration' tab is active. The page displays the following information:

NetScaler SDX	
System Resources	License Information
Total CPU Cores: 24	Platform: 11542
Total SSL Chips: 16	Maximum Instances: 20
Free SSL Chips: 0	Available Instances: 0
Total Memory (GB): 48	Maximum Throughput (Mbps): 42000
Free Memory (GB): 4	Available Throughput (Mbps): 2000
	Cluster License: No
Hypervisor Information	System Information
Uptime: 3 days 23 hours 02 minutes	Platform: 11542
Edition: Citrix XenServer	Product: NetScaler SDX
Version: 5.1	Build: 10.1: Build 129.8, Date: Jul 17 2014, 11:29:34
iSCSI IQN: iqn.2014-10.com.example:193cdfbf	IP Address: 10.0.2.22
Product Code: 6037-6291-7053-f060-72e4-081f	Host ID: 022590d2148
Serial Number: 644aad1e-971e-1dc7-561c-3d05d1f8b92c	System ID: 450170
Build Date: 2014-04-17	Serial Number: 2N5H02E4FX
Build Number: 59235p	System Time: Mon Oct 13 17:24:07 UTC 2014
Supplemental Pack: version 6.1.0-2.6.32.43-0.4.1.xs1.6.10.777.170770xen, build 100015	Uptime: 3 days 22 hours 58 minutes
Kernel Version: 2.6.32.43-0.4.1.xs1.6.10.777.170770xen	BIOS Version: 4.2a

3. Select the System node and, under Set Up Appliance, click Network Configuration to modify the IP address of the Management Service.
4. In the Configure Network Configuration dialog box, specify the following details:
 - 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 XenServer hypervisor.
 - Management Service IP Address*—The IP address of the Management Service.
 - Netmask*—The subnet mask 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 mandatory parameter
5. Click OK.
6. Connect the NetScaler SDX appliance to a switch to access it through the network. Browse to the IP address used above and log on with the default credentials.
7. Apply the new licenses. For instructions, see [NetScaler SDX Licensing Overview](#).
8. Navigate to Configuration > System and, in the System Administration group, click Reboot Appliance. Click Yes to

confirm. You are now ready to provision the VPX instances on the NetScaler SDX appliance. For instructions, see [Provisioning NetScaler Instances](#).

Converting a NetScaler MPX 8200/8400/8600/8800 Appliance to a NetScaler SDX 8400/8600 Appliance

Jan 07, 2014

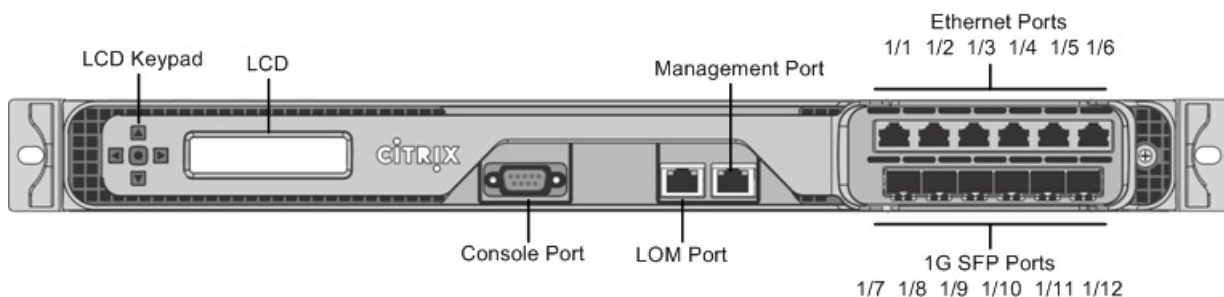
To convert a NetScaler 8200/8400/8600/8800 appliance to a NetScaler SDX 8400/8800 appliance, you must access the appliance through a console cable attached to a computer or terminal.

Before connecting the console cable, configure the computer or terminal to support the following configuration:

1. VT100 terminal emulation
2. 9600 baud
3. 8 data bits
4. 1 stop bit
5. Parity and flow control set to NONE

To convert a NetScaler MPX 8200/8400/8600/8800 appliance to a NetScaler SDX 8400/8600 appliance:

1. Connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.
Note: To use a cable with an RJ45 converter, insert the optional converter into the console port and attach the cable to it.

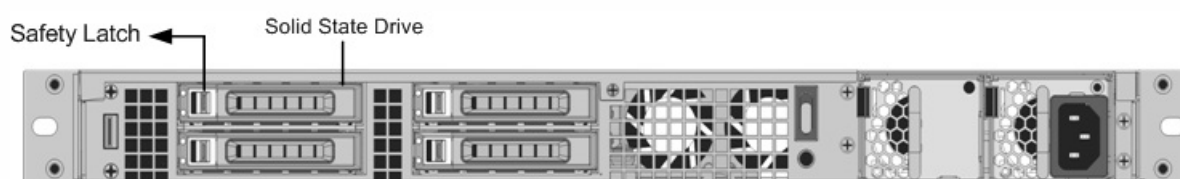


2. On the NetScaler MPX appliance, verify that the solid state drive, power supplies, CPU, SSL cores, and interfaces are operational.
3. Access the console port and enter the administrator credentials.
4. Run the following command from the NetScaler command line interface to display the serial number and confirm the SYSID of the appliance: `> show hardware`
5. Run the following command to display the status of the active interfaces: `> show interface`
6. In the show interface command's output, verify that all of the interfaces are enabled and the status of every interface is shown as UP/UP.
Note: If you have only a limited number of SFP+ transceivers, verify the interfaces in stages. After checking the first set of interfaces, unplug the SFP+ transceivers and plug them in to the next set of ports. The SFP+ transceivers are not hot-swappable. Therefore, restart the MPX appliance after you connect the transceivers.
7. Run the following commands for each of the interfaces:
`> enable interface 1/x`

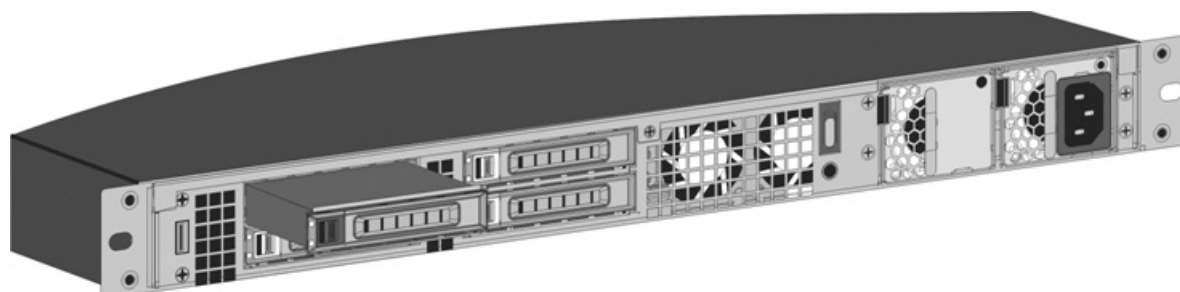
`> enable interface 10/x`

where x is the new interface number.

8. For any interface that you do not want to use after conversion, run the following commands:
 - > disable interface 1/x
 - > disable interface 10/x
9. Run the following command to verify that the status of the power supplies is normal: > stat system –detail
10. Run the following command: > show techsupport
 - Note: The output of the command is available in the /var/tmp/support/collector_<IP_address>_P_<date>.tar.gz file. Copy this file to another computer for future reference. It might be helpful if you want to contact a Citrix technical support engineer.
11. At the NetScaler command line interface, switch to the shell prompt. Type: **shell**
12. Run the following command to verify that 4 Cavium cores are available: **root@ns# dmesg | grep cavium**
13. Run the following command to verify that 132 MB of RAM is reserved for shared memory: **root@ns# dmesg | grep memory**
14. Run the following command to verify that the appliance has 4 CPU cores: **root@ns# dmesg | grep cpu**
15. Run the following command to verify that the /var drive is mounted as /dev/ad4s1e: **root@ns# df -h**
16. Enter the following command to run the ns_hw_err.bash script. This script checks for latent hardware errors. **root@ns# /netscaler/ns_hw_err.bash**
17. At the shell prompt, switch to the NetScaler command line interface. Type: **exit**
18. Run the following command to shut down the appliance: shutdown -p now
19. Locate the solid-state drive on the back panel of the appliance, as shown in the following figure:



20. Verify that the replacement solid-state drive is the one required for your NetScaler model. The Citrix label is on the top of the solid-state drive, which is pre-populated with a new version of BIOS and a recent build of the required Service VM software.
21. Remove the currently installed SSD drive by pushing the safety latch of the drive cover to the right and removing the drive handle and the existing drive.
22. Open the drive handle on the new drive completely to the left, and insert the drive into the slot. The following figure shows the drive partially inserted. Push the drive all the way into the slot.



23. Close the handle flush with the rear side of the appliance so that the solid-state drive locks securely into the slot. Important: The orientation of the solid-state drive is important. Make sure that the Citrix product label is facing up when you insert the drive.

24. Store the old SSD.
25. Start the NetScaler appliance. It takes approximately 30 minutes for the conversion process to complete. The conversion process updates the BIOS, installs the XenServer hypervisor and the Service VM operating system, and copies the NetScaler VPX image to the solid state drive for instance provisioning. When the conversion begins, the LCD screen on the front panel indicates **NSMPX-8200 Booting...** or **NSMPX-8200 10G Booting...** depending on the model of the appliance. When the conversion is successful, the LCD indicates **Citrix NSSDX-8200** or **Citrix NSSDX-8200 10G**, depending on the model of the appliance.
Note: The serial number of the appliance remains the same.
26. Keep the console cable attached during the conversion process. Allow the process to continue until the **netScaler-sdx login:** prompt appears.
27. When the appliance finishes the conversion process, it no longer has the previously working configuration. Therefore, you can access the appliance through a Web browser only. Use the default IP address: 192.168.100.1/16. Configure a computer on network 192.168.0.0 and connect it directly to the management port 0/1 of the appliance by using a cross-over Ethernet cable, or access the NetScaler SDX appliance through a network hub by using a straight-through Ethernet cable. Use the default credentials. (**Username:** nsroot and **Password:** nsroot).
28. Select the Configuration tab.
29. Verify that the System Resource section displays 8 CPU cores, 4 SSL cores, and 32 GB of total memory for the NetScaler SDX appliance.
30. Select System node and click the Network Configuration link on the System page to modify the IP address of the Service VM.
31. In the Modify Network Configuration dialog box, specify the following details:
 1. Interface—The interface through which clients connect to the Management Service. Possible values: 0/1, 0/2. Default: 0/1.
 2. XenServer IP Address—The IP address of XenServer hypervisor.
 3. Management Service IP Address—The IP address of the Management Service.
 4. Netmask—The subnet mask for the subnet in which the SDX appliance is located.
 5. Gateway—The default gateway for the network.
 6. DNS Server*—The IP address of the DNS server.*An optional parameter
32. Click OK.
33. Connect the NetScaler SDX appliance to a switch to access it through the network. Browse to the Management Service IP address defined in step 31 and log on with the default credentials.
34. For instructions for applying the licenses, see [NetScaler SDX Licensing Overview](#).
Note: After the conversion is complete, the LCD display might display **CITRIX/NetScaler SDX**. If so, you must switch off the appliance through the Service VM so that, after you power the appliance back on, it displays **Citrix NSSDX-8200** or **Citrix NSSDX-8200 10G**. On the Service VM configuration page, in the System section, click the Shut Down Appliance link. If the green LED light of the power supply, located on the back of the appliance, blinks, the appliance is completely shut down.

Converting a NetScaler MPX 14020/14030/14040/14060/14080/14100 Appliance to a NetScaler SDX 14020/14030/14040/ 14060/14080/14100 Appliance

Dec 04, 2015

You can convert a NetScaler MPX appliance to a NetScaler SDX appliance by upgrading the software through a new Solid State Drive (SSD). Citrix supplies a field conversion kit to migrate a NetScaler MPX appliance to a NetScaler SDX appliance.

The conversion requires minimum of four SSDs.

Note: Citrix recommends that you configure the Lights Out Management (LOM) Port of the NetScaler appliance before starting the conversion process. For more information on the LOM port of the NetScaler appliance, see [Lights Out Management Port of the NetScaler Appliance](#).

To convert a NetScaler MPX appliance to a NetScaler SDX appliance, you must access the appliance through a console cable attached to a computer or terminal. Before connecting the console cable, configure the computer or terminal to support the following configuration:

- VT100 terminal emulation
- 9600 baud
- 8 data bits
- 1 stop bit
- Parity and flow control set to NONE

Connect one end of the console cable to the RS232 serial port on the appliance, and the other end to the computer or terminal.

Note: To use a cable with an RJ-45 converter, insert the optional converter into the console port and attach the cable to it.

Citrix recommends you to connect a VGA monitor to the appliance to monitor the conversion process, because the LOM connection is be lost during the conversion process.

With the cable attached, verify that the MPX appliance's components are functioning correctly. You are then ready to begin the conversion. The conversion process modifies the Basic Input-Output System (BIOS), installs XenServer hypervisor and a Service Virtual Machine image, and copies the NetScaler VPX image to the Solid State Drive.

The conversion process also sets up a Redundant Array of Independent Disks (RAID) controller for local storage (SSD slot # 1 and SSD slot # 2) and Netscaler VPX storage (SSD slot # 3 and SSD slot # 4).

After the conversion process, you make a few modifications to the appliance's configuration and apply a new license. You can then provision the VPX instances through the Management Service on what is now a NetScaler SDX appliance.

To verify proper operation of the MPX appliance's components

1. Access the console port and enter the administrator credentials.
2. Run the following command from the command line interface of the appliance to display the serial number: show hardware

The serial number might be helpful in the event that you want to contact Citrix Technical Support.

Example

```
> show hardware

Platform: NSMPX-14000 12*CPU+16*IX+2*E1K+2*CVM N3 250101

Manufactured on: 10/2/2015

CPU: 2600MHZ

Host Id: 234913926

Serial no: JSW4UCKKM5

Encoded serial no: JSW4UCKKM5

Done

>
```

3. Run the following command to display the status of the active 10G interfaces: show interface

4. In the show interface command's output, verify that all of the interfaces are enabled and the status of every interface is shown as UP/UP.

Note: If you do not have an SFP+ transceiver for every port, verify the interfaces in stages. After checking the first set of interfaces, unplug the SFP+ transceivers and plug them in to the next set of ports.

5. Run the following command for each of the interfaces that are not in the UP/UP state:

```
*enable interface 10/x
```

where x is the new interface number.

6. Run the following command to verify that the status of the power supplies is normal: stat system -detail

7. Run the following command to generate a tar of system configuration data and statistics: show techsupport

Note: The output of the command is available in the /var/tmp/support /collector_<IP_address>_P_<date>.tar.gz file. Copy this file to another computer for future reference. The output of the command might be helpful in the event that you want to contact Citrix Technical Support.

8. At the NetScaler command line interface, switch to the shell prompt. Type: **shell**

9. Run the following command to verify the number of Cavium cards available depending upon your appliance:

```
root@ns# grep "cavium" /var/nslog/dmesg.boot
```

Example

```
root@ns# grep "cavium" /var/nslog/dmesg.boot

Cavium cavium_probe : found card 0x177d,device=0x11

cavium0 mem 0xdd600000-0xdd6fffff irq 32 at device 0.0 on pci3

Cavium cavium_probe : found card 0x177d,device=0x11

cavium1 mem 0xfaa00000-0xfaafffff irq 64 at device 0.0 on pci136
```


10. Run the following command to verify the RAM memory reserved for shared memory depending upon your appliance:

root@ns# grep "memory" /var/nslog/dmesg.boot

Example

```
root@ns# grep "memory" /var/nslog/dmesg.boot
real memory = 70866960384 (67584 MB)
avail memory = 66267971584 (63198 MB)
```

11. Run the following command to verify the number of CPU cores depending upon your appliance :

root@ns# grep "cpu" /var/nslog/dmesg.boot

Example

```
root@ns# grep "cpu" /var/nslog/dmesg.boot
cpu0 (BSP): APIC ID: 0
cpu1 (AP): APIC ID: 2
cpu2 (AP): APIC ID: 4
cpu3 (AP): APIC ID: 6
cpu4 (AP): APIC ID: 8
cpu5 (AP): APIC ID: 10
cpu6 (AP): APIC ID: 32
cpu7 (AP): APIC ID: 34
cpu8 (AP): APIC ID: 36
cpu9 (AP): APIC ID: 38
cpu10 (AP): APIC ID: 40
cpu11 (AP): APIC ID: 42
cpu0: <ACPI CPU> on acpi0
acpi_throttle0: <ACPI CPU Throttling> on cpu0
cpu1: <ACPI CPU> on acpi0
acpi_throttle1: <ACPI CPU Throttling> on cpu1
```

```
cpu2: <ACPI CPU> on acpi0
acpi_throttle2: <ACPI CPU Throttling> on cpu2
cpu3: <ACPI CPU> on acpi0
acpi_throttle3: <ACPI CPU Throttling> on cpu3
cpu4: <ACPI CPU> on acpi0
acpi_throttle4: <ACPI CPU Throttling> on cpu4
cpu5: <ACPI CPU> on acpi0
acpi_throttle5: <ACPI CPU Throttling> on cpu5
cpu6: <ACPI CPU> on acpi0
acpi_throttle6: <ACPI CPU Throttling> on cpu6
cpu7: <ACPI CPU> on acpi0
acpi_throttle7: <ACPI CPU Throttling> on cpu7
cpu8: <ACPI CPU> on acpi0
acpi_throttle8: <ACPI CPU Throttling> on cpu8
cpu9: <ACPI CPU> on acpi0
acpi_throttle9: <ACPI CPU Throttling> on cpu9
cpu10: <ACPI CPU> on acpi0
acpi_throttle10: <ACPI CPU Throttling> on cpu10
cpu11: <ACPI CPU> on acpi0
acpi_throttle11: <ACPI CPU Throttling> on cpu11
root@ns#
```

12. Run the following command to verify that the /var drive is mounted as /dev/ad8s1e: root@ns# df -h

13. Run the following command to execute the ns_hw_err.bash script, which checks for latent hardware errors: root@ns# ns_hw_err.bash

Example

```
root@ns# ns_hw_err.bash
NetScaler NS10.1: Build 133.11.nc, Date: Sep 21 2015, 17:59:51
platform: serial JSW4UCKKM5
platform: sysid 250101 - NSMPX-14000 12*CPU+16*IX+2*E1K+2*CVM N3
HDD MODEL: ar0: 227328MB <Intel MatrixRAID RAID1> status: READY
```

```

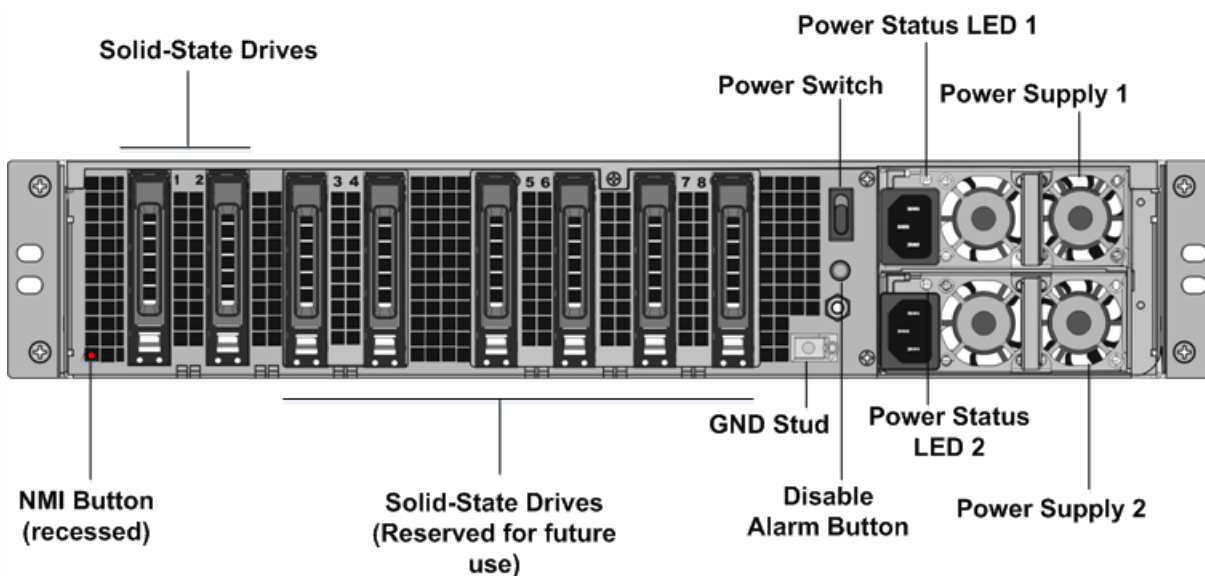
Generating the list of newnslog files to be processed...
Generating the events from newnslog files...
Checking for HDD errors...
Checking for HDD SMART errors...
Checking for Flash errors...
/var/nslog/dmesg.prev:* DEVELOPER mode - run NetScaler manually! *
*****
FOUND    1 Flash errors: DEVELOPER mode - run NetScaler manually
*****
Checking for SSL errors...
Checking for BIOS errors...
Checking for SMB errors...
Checking for MotherBoard errors...
Checking for CMOS errors...
    License year: 2015: OK
License server failed at startup. Check /var/log/license.log
Vendor daemon failed at startup. Check /var/log/license.log
Checking for SFP/NIC errors...
Checking for Firmware errors...
Checking for License errors...
Checking for Undetected CPUs...
Checking for DIMM flaps...
Checking for LOM errors...
Checking the Power Supply Errors...
root@ns#

```

14. Important: Physically disconnect all ports except the LOM port, including the management port, from the network.
15. At the shell prompt, switch to the NetScaler command line. Type: exit
16. Run the following command to shut down the appliance: shutdown -p now

To upgrade the appliance

1. Power off the NetScaler appliance.
2. Locate two solid-state drives (SSDs) on the back of the appliance in slot #1 and slot #2, as shown in the following figure:



3. Verify that the replacement solid-state drives (SSDs) are the ones required for your NetScaler model. The conversion requires minimum of four SSDs. The Citrix label is on the top of one of the solid-state drives, which is pre-populated with a new version of BIOS and a recent build of the required NetScaler SDX Management Service. This SSD must be installed in slot # 1.

4. Remove the SSDs by pushing the safety latch of the drive cover down while pulling the drive handle.

5. On the new Citrix Certified SSD drive, open the drive handle completely to the left, and then insert the new drive into the slot #1 as far as possible.

6. To seat the drive, close the handle flush with the rear side of the appliance so that the drive locks securely into the slot.

Important: The orientation of the SSD is important. When you insert the drive, make sure that the Citrix product label is at the top.

7. Insert a second Citrix certified SSD, which matches the capacity of the SSD in slot #1, in slot # 2. Insert additional blank Citrix certified SSDs in slots #3 and #4.

Note: If the license of your appliance is 14040, insert additional blank Citrix certified SSDs in slots #3, #4, #5, and #6.

If the license of your appliance is 14060/14080/14100, insert additional blank Citrix certified SSDs in slots #3, #4, #5, #6, #7, and #8.

Important: Note that mixing and matching of old and new SSDs is not supported. SSDs in slot #1 and slot # 2, which constitute the first RAID pair (local storage), must be of same size and type. Similarly, SSDs in slot # 3 and slot # 4, which constitute the second RAID pair (VPX storage), must be of same size and type. Do not use any other drives that are not part of the provided conversion kit.

8. Store the old SSDs for future handling.

9. Disconnect all network cables from the data ports and the management ports.

10. Start the NetScaler appliance. For instructions, see “Switching on the Appliance” in [Installing the Hardware](#).

The conversion process can run for approximately 30 minutes, during which you must not power cycle the appliance. The entire conversion process might not be visible on the console and might appear to be unresponsive.

The conversion process updates the BIOS, installs the XenServer hypervisor and the Management Service Operating system, and copies the NetScaler VPX image to the SSD for instance provisioning, and forms the Raid1 pair.

Note: The serial number of the appliance remains the same.

11. Keep the console cable attached during the conversion process. Allow the process to complete, at which point the netScaler-sdx login: prompt appears.
12. During the conversion process the LOM port connection may be lost as it resets the IP address to the default value of 192.168.1.3. The conversion status output is available on the VGA monitor.
13. To make sure that the conversion is successful, verify that the FVT result indicates success. Run the following command:
tail /var/log/fvt/fvt.log

Example

```
[root@netScaler-sdx ~]# tail /var/log/fvt/fvt.log
Wed, 28 Oct 2015 04:40:47 /opt/xenSource/packages/files/fvt/workers/check_vf_count --pf_device="0000:89:00.1" --vf_count="40"
Wed, 28 Oct 2015 04:40:47 => PASS

Wed, 28 Oct 2015 04:40:47 /opt/xenSource/packages/files/fvt/workers/check_vf_count --pf_device="0000:03:00.0" --vf_count="8"
Wed, 28 Oct 2015 04:40:47 => PASS

Wed, 28 Oct 2015 04:40:47 /opt/xenSource/packages/files/fvt/workers/check_vf_count --pf_device="0000:88:00.0" --vf_count="8"
Wed, 28 Oct 2015 04:40:47 => PASS

Wed, 28 Oct 2015 04:40:47 FVT RESULT: SUCCESS!
[root@netScaler-sdx ~]#
```

To reconfigure the converted appliance

After the conversion process, the appliance no longer has its previous working configuration. Therefore, you can access the appliance through a web browser only by using the default IP address: 192.168.100.1/16. Configure a computer on network 192.168.0.0 and connect it directly to the appliance's management port (0/1) with a cross-over Ethernet cable, or access the NetScaler SDX appliance through a network hub by using a straight through Ethernet cable. Use the default credentials to log on (Username: nsroot and Password: nsroot), and then do the following:

1. Select the Configuration tab.
2. Verify that the System Resource section displays the accurate number of CPU cores, SSL cores, and the total memory for your NetScaler SDX appliance.
3. Select the System node and, under Set Up Appliance, click Network Configuration to modify the IP address of the Management Service.
4. In the Configure Network Configuration dialog box, specify the following details:
 - 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 XenServer hypervisor.
 - Management Service IP Address*—The IP address of the Management Service.
 - Netmask*—The subnet mask 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 mandatory parameter

5. Click OK. Connection to the Management Service is lost as the network information was changed.
6. Connect the NetScaler SDX appliance's management port 0/1 to a switch to access it through the network. Browse to the IP address used above and log on with the default credentials.
1. Apply the new licenses. For instructions, see [NetScaler SDX Licensing Overview](#).

Navigate to Configuration > System and, in the System Administration group, click Reboot Appliance. Click Yes to confirm. You are now ready to provision the VPX instances on the NetScaler SDX appliance. For instructions, see [Provisioning NetScaler Instances](#).

Converting a NetScaler MPX 24100 and 24150 Appliance to a NetScaler SDX 24100 and 24150 Appliance

Apr 12, 2016

You can convert a NetScaler MPX appliance to a NetScaler SDX appliance by upgrading the software through a new Solid State Drive (SSD). Citrix supplies a field conversion kit to migrate a NetScaler MPX appliance to a NetScaler SDX appliance.

The conversion requires minimum of four SSDs.

Note: Citrix recommends that you configure the Lights Out Management (LOM) Port of the NetScaler appliance before starting the conversion process. For more information on the LOM port of the NetScaler appliance, see [Lights Out Management Port of the NetScaler Appliance](#).

To convert a NetScaler MPX appliance to a NetScaler SDX appliance, you must access the appliance through a console cable attached to a computer or terminal. Before connecting the console cable, configure the computer or terminal to support the following configuration:

- VT100 terminal emulation
- 9600 baud
- 8 data bits
- 1 stop bit
- Parity and flow control set to NONE

Connect one end of the console cable to the RS232 serial port on the appliance, and the other end to the computer or terminal.

Note: To use a cable with an RJ-45 converter, insert the optional converter into the console port and attach the cable to it.

Citrix recommends you to connect a VGA monitor to the appliance to monitor the conversion process, because the LOM connection is be lost during the conversion process.

With the cable attached, verify that the MPX appliance's components are functioning correctly. You are then ready to begin the conversion. The conversion process modifies the Basic Input-Output System (BIOS), installs XenServer hypervisor and a Service Virtual Machine image, and copies the NetScaler VPX image to the Solid State Drive.

The conversion process also sets up a Redundant Array of Independent Disks (RAID) controller for local storage (SSD slot # 1 and SSD slot # 2) and Netscaler VPX storage (SSD slot # 3 and SSD slot # 4).

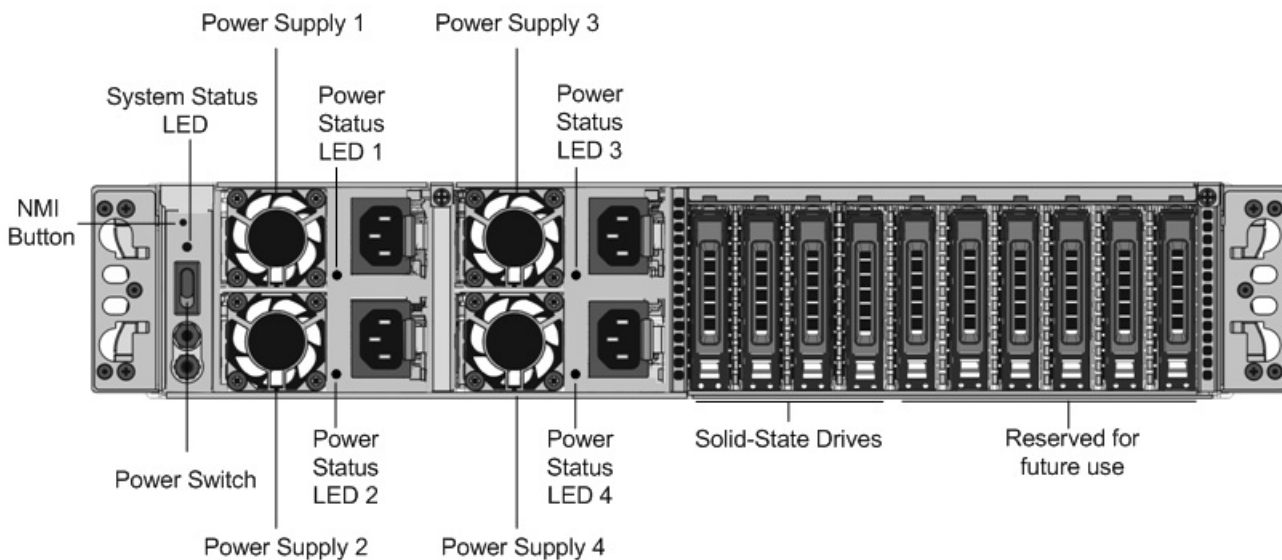
After the conversion process, you make a few modifications to the appliance's configuration and apply a new license. You can then provision the VPX instances through the Management Service on what is now a NetScaler SDX appliance.

To verify proper operation of the MPX appliance's components

1. Access the console port and enter the administrator credentials.
2. Run the following command from the command line interface of the appliance to display the serial number:
show hardware
The serial number might be helpful in the event that you want to contact Citrix Technical Support.
3. Run the following command to display the status of the active 10G interfaces: show interface
4. In the show interface command's output, verify that all of the interfaces are enabled and the status of every interface is shown as UP/UP.
Note: If you do not have an SFP+ transceiver for every port, verify the interfaces in stages. After checking the first set of interfaces, unplug the SFP+ transceivers and plug them in to the next set of ports.
5. Run the following command for each of the interfaces that are not in the UP/UP state:
 - o enable interface 10/x
 - o enable interface 1/x
 where x is the new interface number.
6. Run the following command to verify that the status of the power supplies is normal: stat system -detail
7. Run the following command to generate a tar of system configuration data and statistics: show techsupport
Note: The output of the command is available in the /var/tmp/support/collector_<IP_address>_P_<date>.tar.gz file. Copy this file to another computer for future reference. The output of the command might be helpful in the event that you want to contact Citrix Technical Support.
8. At the NetScaler command line interface, switch to the shell prompt. Type: shell
9. Run the following command to verify the number of Cavium cards available depending upon your appliance:
root@ns# grep "cavium" /var/nslog/dmesg.boot
10. Run the following command to verify the RAM memory reserved for shared memory depending upon your appliance:
root@ns# grep "memory" /var/nslog/dmesg.boot
11. Run the following command to verify the number of CPU cores depending upon your appliance :
root@ns# grep "cpu" /var/nslog/dmesg.boot
12. Run the following command to verify that the /var drive is mounted as /dev/ad8s1e: root@ns# df -h
13. Run the following command to execute the ns_hw_err.bash script, which checks for latent hardware errors: root@ns# ns_hw_err.bash
14. Important: Physically disconnect all ports except the LOM port, including the management port, from the network.
15. At the shell prompt, switch to the NetScaler command line. Type: exit
16. Run the following command to shut down the appliance: shutdown -p now

To upgrade the appliance

1. Power off the NetScaler appliance.
2. Locate two solid-state drives (SSDs) on the back of the appliance in slot #1 and slot #2, as shown in the following figure:



3. Verify that the replacement solid-state drives (SSDs) are the ones required for your NetScaler model. The conversion requires minimum of four SSDs. The Citrix label is on the top of one of the solid-state drives, which is pre-populated with a new version of BIOS and a recent build of the required NetScaler SDX Management Service. This SSD must be installed in slot # 1.

4. Remove the SSDs by pushing the safety latch of the drive cover down while pulling the drive handle.

5. On the new Citrix Certified SSD drive, open the drive handle completely to the left, and then insert the new drive into the slot #1 as far as possible.

6. To seat the drive, close the handle flush with the rear side of the appliance so that the drive locks securely into the slot.

Important: The orientation of the SSD is important. When you insert the drive, make sure that the Citrix product label is at the top.

7. Insert a second Citrix certified SSD, which matches the capacity of the SSD in slot #1, in slot # 2. Insert additional blank Citrix certified SSDs in slots #3 and #4.

Important: Note that mixing and matching of old and new SSDs is not supported. SSDs in slot #1 and slot # 2, which constitute the first RAID pair (local storage), must be of same size and type. Similarly, SSDs in slot # 3 and slot # 4, which constitute the second RAID pair (VPX storage), must be of same size and type. Do not use any other drives that are not part of the provided conversion kit.

8. Disconnect all network cables from the data ports and the management ports.

9. Start the NetScaler appliance. For instructions, see “Switching on the Appliance” in Installing the Hardware.

The conversion process can run for approximately 30 minutes, during which you must not power cycle the appliance. The entire conversion process might not be visible on the console and might appear to be unresponsive.

The conversion process updates the BIOS, installs the XenServer hypervisor and the Management Service Operating system, and copies the NetScaler VPX image to the SSD for instance provisioning, and forms the Raid1 pair.

Note: The serial number of the appliance remains the same.

10. Keep the console cable attached during the conversion process. Allow the process to complete, at which point the netscaler-sdx login: prompt appears.

11. During the conversion process the LOM port connection may be lost as it resets the IP address to the default value of 192.168.1.3. The conversion status output is available on the VGA monitor.

Third-Party Virtual Machines

Jun 20, 2013

The NetScaler SDX appliance supports provisioning of the following third-party virtual machines (instances):

- SECUREMATRIX GSB
- Websense Protector
- BlueCat DNS/DHCP Server
- CA Access Gateway
- PaloAlto VM-Series

SECUREMATRIX GSB provides a highly secure password system that eliminates the need to carry any token devices. Websense Protector provides monitoring and blocking capabilities, preventing data loss and leaks of sensitive information. BlueCat DNS/DHCP Server delivers DNS and DHCP for your network. PaloAlto VM-Series on Citrix NetScaler SDX enables consolidation of advanced security and ADC capabilities on a single platform, for secure, reliable access to applications by businesses, business units, and service-provider customers. The combination of VM-Series on Citrix NetScaler SDX also provides a complete, validated, security and ADC solution for Citrix XenApp and XenDesktop deployments.

You can provision, monitor, manage, and troubleshoot an instance from the Management Service. All the above third-party instances use the SDXTools daemon to communicate with the Management Service. The daemon is pre-installed on the provisioned instance. You can upgrade the daemon when new versions become available.

Note: The total number of instances that you can provision on an NetScaler SDX appliance depends on the license installed on the appliance.

Important! You must upgrade your XenServer version to version 6.1.0 before you install any third-party instance.

SECUREMATRIX GSB

Jan 31, 2011

SECUREMATRIX is a highly secure, tokenless, one-time-password (OTP) authentication solution that is easy to use and cost effective. It uses a combination of location, sequence, and image pattern from a matrix table to generate a single-use password. SECUREMATRIX GSB server with SECUREMATRIX Authentication server substantially enhances the security of VPN/SSL-VPN endpoints, cloud based applications and resources, desktop/virtual desktop login, and web applications (Reverse proxy with OTP), providing a solution that is compatible with PCs, Virtual Desktops, tablets, and smart phones.

Utilizing the NetScaler SDX multitenant platform architecture in a software defined network (SDN), SECUREMATRIX's strong authentication feature can be easily combined or integrated with other tenants or cloud services delivered through the NetScaler, such as Web Interface, XenApp, XenDesktop, and many other application services that require authentication.

For more information about SECUREMATRIX, see <http://www.csessi.com/>.

SECUREMATRIX GSB requires a SECUREMATRIX Authentication server that must be configured outside the SDX appliance. Select exactly one interface and specify the network settings for only that interface.

Note: SR-IOV interfaces (1/x and 10/x) that are part of a channel do not appear in the list of interfaces because channels are not supported on a SECUREMATRIX GSB instance.

You must download an XVA image from the SECUREMATRIX website and upload it to the SDX appliance before you start provisioning the instance. For more information about downloading an XVA image, see the SECUREMATRIX website. Make sure that you are using Management Service build 118.7 or later on the NetScaler SDX appliance.

On the Configuration tab, navigate to SECUREMATRIX GSB > Software Images.

To upload an XVA image to the SDX appliance

1. In the details pane, under XVA Files > Action, click Upload.
2. In the dialog box that appears, click Browse, and then select the XVA file that you want to upload.
3. Click Upload. The XVA file appears in the XVA Files pane.

To provision a SECUREMATRIX instance

1. On the Configuration tab, navigate to SECUREMATRIX GSB > Instances.
2. In the details pane, click Add.
3. In the Provision SECUREMATRIX GSB wizard, follow the instructions on the screen.
4. Click Finish, and then click Close.

After you provision the instance, log on to the instance and perform detailed configuration. For more information, see [the SECUREMATRIX website](#).

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

Note: If you modify any of the interface parameters or the name of the instance, the instance stops and restarts to put

the changes into effect.

You can generate a tar archive for submission to technical support. For information about generating a technical support file, see [Generating a Tar Archive for Technical Support](#).

You can also back up the configuration of a SECUREMATRIX GSB instance and later use the backup data to restore the configuration of the instance on the SDX appliance. For information about backing up and restoring an instance, see [Backing Up and Restoring the Configuration Data of the SDX Appliance](#).

The SDX appliance collects statistics, such as the version of SDXTools, the states of SSH and CRON daemons, and the Webserver state, of a SECUREMATRIX GSB instance.

To view the statistics related to a SECUREMATRIX GSB instance

1. Navigate to SECUREMATRIX GSB > Instances.
2. In the details pane, click the arrow next to the name of the instance.

You can start, stop, restart, force stop, or force restart a SECUREMATRIX GSB instance from the Management Service.

On the Configuration tab, expand SECUREMATRIX GSB.

To start, stop, restart, force stop, or force restart an instance

1. Click Instances.
2. In the details pane, select the instance on which you want to perform the operation, and then select one of the following options:
 - Start
 - Shut Down
 - Reboot
 - Force Shutdown
 - Force Reboot
3. In the Confirm message box, click Yes.

SDXTools, a daemon running on the SECUREMATRIX GSB instance, is used for communication between the Management Service and the instance.

Upgrading SDXTools involves uploading the file to the SDX appliance, and then upgrading SDXTools after selecting an instance. You can upload an SDXTools file from a client computer to the SDX appliance.

To upload an SDXTools file

1. In the navigation pane, expand Management Service, and then click SDXTools Files.
2. In the details pane, from the Action list, select Upload.
3. In the Upload SDXTools Files dialog box, click Browse, navigate to the folder that contains the file, and then double-click the file.
4. Click Upload.

To upgrade SDXTools

On the Configuration tab, expand SECUREMATRIX GSB.

1. Click Instances.
2. In the details pane, select an instance.
3. From the Action list, select Upgrade SDXTools.
4. In the Upgrade SDXTools dialog box, select a file, click OK, and then click Close.

The process of upgrading the SECUREMATRIX GSB instance involves uploading the software image of the target build to the SDX appliance, and then upgrading the instance. Downgrading loads an earlier version of the instance.

On the Configuration tab, expand SECUREMATRIX GSB.

To upload the software image

1. Click Software Images.
2. In the details pane, from the Action list, select Upload.
3. In the dialog box, click Browse, navigate to the folder that contains the build file, and then double-click the build file.
4. Click Upload.

To upgrade the instance

1. Click Instances.
2. In the details pane, select an instance.
3. From the Action list, select Upgrade.
4. In the dialog box that appears, select a file, click OK, and then click Close.

To downgrade an instance

Updated: 2013-06-18

1. Click Instances.
2. In the details pane, select an instance.
3. From the Action list, select Downgrade.
4. In the Confirm message box, click Yes.

You can ping a SECUREMATRIX GSB instance from the Management Service to check whether the device is reachable. You can trace the route of a packet from the Management Service to an instance to determine the number of hops involved in reaching the instance.

You can rediscover an instance to view the latest state and configuration of an instance. During rediscovery, the Management Service fetches the configuration and the version of the SECUREMATRIX GSB running on the SDX appliance. By default, the Management Service schedules instances for rediscovery once every 30 minutes.

On the Configuration tab, expand SECUREMATRIX GSB.

To ping an instance

1. Click Instances.
2. In the details pane, select the instance that you want to ping, and from the Action list, click Ping. The Ping message box shows whether the ping is successful.

To trace the route of an instance

1. Click Instances.
2. In the details pane, select the instance for which you want to trace the route, and from the Action list, click TraceRoute. The Traceroute message box displays the route to the instance.

To rediscover an instance

1. Click Instances.
2. In the details pane, select the instance that you want to rediscover, and from the Action list, click Rediscover.
3. In the Confirm message box, click Yes.

Websense Protector

Jan 31, 2011

The Websense© Data Security protector is a virtual machine that intercepts outbound HTTP traffic (posts) and analyzes it to prevent data loss and leaks of sensitive information over the web. The protector communicates with a dedicated Windows server for DLP policy information and can monitor or block data from being posted when a match is detected. Content analysis is performed on box, so no sensitive data leaves the protector during this process.

To use the protector's data loss prevention (DLP) capabilities, you must purchase and install Websense Data Security, configure Web DLP policies in the Data Security manager, and perform initial set up through the Management Service.

For more information about the Websense Protector, see

http://www.websense.com/content/support/library/data/v773/citrix_prot/first.aspx .

The Websense© Protector requires a Data Security Management Server that must be configured outside the SDX appliance. Select exactly one management interface and two data interfaces. For the data interfaces, you must select Allow L2 Mode. Make sure that the Data Security Management Server can be accessed through the management network of the Websense protector. For the Name Server, type the IP address of the domain name server (DNS) that will serve this protector.

Note: SR-IOV interfaces (1/x and 10/x) that are part of a channel do not appear in the list of interfaces because channels are not supported on a Websense protector instance.

You must download a protector image from the Websense website and upload it to the SDX appliance before you start provisioning the instance. For more information about downloading a protector image, see the [Websense website](#) . Make sure that you are using Management Service build 118.7 or later on the NetScaler SDX appliance.

On the Configuration tab, navigate to Websense Protector > Software Images.

To upload an XVA image to the SDX appliance

1. In the details pane, under XVA Files > Action, click Upload.
2. In the dialog box that appears, click Browse, and then select the XVA file that you want to upload.
3. Click Upload. The XVA file appears in the XVA Files pane.

To provision a Websense protector instance

1. On the Configuration tab, navigate to Websense Protector > Instances.
2. In the details pane, click Add.
3. In the Provision Websense Protector wizard, follow the instructions on the screen.
4. Click Finish, and then click Close.

After you provision the instance, log on to the instance and perform detailed configuration. For more information, see the [Websense website](#).

To modify the values of the parameters of a provisioned Websense protector instance, in the Websense Protector Instances pane, select the instance that you want to modify, and then click Modify. In the Modify Websense Protector wizard, set the parameters. Do not modify the interfaces that were selected at the time of provisioning a Websense

instance. XVA file cannot be changed unless you delete the instance and provision a new one.

You can generate a tar archive for submission to technical support. For information about generating a technical support file, see [Generating a Tar Archive for Technical Support](#).

The SDX appliance collects statistics, such as the version of SDXTools, the status of the Websense© Data Security policy engine, and the Data Security proxy status, of a Websense protector instance.

To view the statistics related to a Websense protector instance

1. Navigate to Websense Protector > Instances.
2. In the details pane, click the arrow next to the name of the instance.

You can start, stop, restart, force stop, or force restart a Websense© protector instance from the Management Service.

On the Configuration tab, expand Websense Protector.

To start, stop, restart, force stop, or force restart a Websense protector instance

1. Click Instances.
2. In the details pane, select the instance on which you want to perform the operation, and then select one of the following options:
 - Start
 - Shut Down
 - Reboot
 - Force Shutdown
 - Force Reboot
3. In the Confirm message box, click Yes.

SDXTools, a daemon running on the third-party instance, is used for communication between the Management Service and the third-party instance.

Upgrading SDXTools involves uploading the file to the SDX appliance, and then upgrading SDXTools after selecting an instance. You can upload an SDXTools file from a client computer to the SDX appliance.

To upload an SDXTools file

1. In the navigation pane, expand Management Service, and then click SDXTools Files.
2. In the details pane, from the Action list, select Upload.
3. In the Upload SDXTools Files dialog box, click Browse, navigate to the folder that contains the file, and then double-click the file.
4. Click Upload.

To upgrade SDXTools

On the Configuration tab, expand Websense Protector.

1. Click Instances.
2. In the details pane, select an instance.
3. From the Action list, select Upgrade SDXTools.
4. In the Upgrade SDXTools dialog box, select a file, click OK, and then click Close.

The process of upgrading the Websense© protector instance involves uploading the software image of the target build to the SDX appliance, and then upgrading the instance.

On the **Configuration** tab, expand **Websense Protector**.

To upload the software image

1. Click Software Images.
2. In the details pane, from the Action list, select Upload.
3. In the dialog box, click Browse, navigate to the folder that contains the build file, and then double-click the build file.
4. Click Upload.

To upgrade the instance

1. Click Instances.
2. In the details pane, select an instance.
3. From the Action list, select Upgrade.
4. In the dialog box that appears, select a file, click OK, and then click Close.

You can ping a Websense© protector instance from the Management Service to check whether the device is reachable. You can trace the route of a packet from the Management Service to an instance to determine the number of hops involved in reaching the instance.

You can rediscover an instance to view the latest state and configuration of an instance. During rediscovery, the Management Service fetches the configuration and the version of the Websense protector running on the SDX appliance. By default, the Management Service schedules instances for rediscovery once every 30 minutes.

On the Configuration tab, expand Websense Protector.

To ping an instance

1. Click Instances.
2. In the details pane, select the instance that you want to ping, and from the Action list, click Ping. The Ping message box shows whether the ping is successful.

To trace the route of an instance

1. Click Instances.
2. In the details pane, select the instance for which you want to trace the route, and from the Action list, click TraceRoute. The Traceroute message box displays the route to the instance.

To rediscover an instance

1. Click Instances.
2. In the details pane, select the instance that you want to rediscover, and from the Action list, click Rediscover.
3. In the Confirm message box, click Yes.

BlueCat DNS/DHCP

Jan 31, 2011

BlueCat DNS/DHCP Server™ is a software solution that can be hosted on the Citrix NetScaler SDX platform to deliver reliable, scalable and secure DNS and DHCP core network services without requiring additional management costs or data center space. Critical DNS services can be load balanced across multiple DNS nodes within a single system or across multiple SDX appliances without the need for additional hardware.

Virtual instances of BlueCat DNS/DHCP Server™ can be hosted on NetScaler SDX to provide a smarter way to connect mobile devices, applications, virtual environments and clouds.

To learn more about BlueCat and Citrix, visit the BlueCat website at <http://www.bluecatnetworks.com/solutions/citrix/>.

To request a free trial version of BlueCat™ DNS/DHCP Server for Citrix Netscaler SDX, visit <http://pages.bluecatnetworks.com/free-trial.html>.

If you are an existing BlueCat customer, you can download software and documentation via the BlueCat support portal at <https://care.bluecatnetworks.com/>.

Updated: 2013-12-03

You must download an XVA image from the Bluecat Customer Care, at <https://care.bluecatnetworks.com>. After you have downloaded the XVA image, upload it to the SDX appliance before you start provisioning the instance. Make sure that you are using Management Service build 118.7 or later on the NetScaler SDX appliance.

Management channel across 0/1 and 0/2 interfaces are supported on BlueCat DNS/DHCP VMs. For more information see [Configuring channel from Management Service](#).

On the Configuration tab, navigate to BlueCat DNS/DHCP > Software Images.

To upload an XVA image to the SDX appliance

1. In the details pane, under XVA Files > Action, click Upload.
2. In the dialog box that appears, click Browse, and then select the XVA file that you want to upload.
3. Click Upload. The XVA file appears in the XVA Files pane.

To provision a BlueCat DNS/DHCP instance

1. On the Configuration tab, navigate to BlueCat DNS/DHCP > Instances.
2. In the details pane, click Add. The Provision BlueCat DNS/DHCP Server page opens.
3. In the Provision BlueCat DNS/DHCP wizard, follow the instructions on the screen.
 - Under Instance Creation, in the Name field, enter a name for the instance and select the uploaded image from the XVA File drop-down menu, then Click Next. Optionally, in the Domain Name field, enter a domain name for the instance.
Note: The name should contain no spaces.
 - Under Network Settings, from the Management Interface drop-down menu, select the interface through which to manage the instance, set the IP address and gateway for that interface. You can assign interfaces explicitly for high

availability and service. Select the parameters and then click **Next**.

Note: When assigning interfaces for management, high availability and service, make sure you assign the interfaces based on supported combination of interfaces:

- You can select the same interface for all three.
- You can select a different interface for all three.
- You can select the same interface for management and service, but select a different interface for high availability.

4. Click Finish, and then click Close. The instance will be created, booted, and configured with the selected IP address.

After you provision the instance, log on to the instance through SSH to complete the configuration. For details on how to configure the BlueCat DNS/DHCP Server or place it under the control of BlueCat Address Manager, see the appropriate BlueCat Administration Guide, available at <https://care.bluecatnetworks.com>.

To modify the values of the parameters of a provisioned BlueCat DNS/DHCP Server instance, from the BlueCat DNS/DHCP Instances pane, select the instance that you want to modify, and then click Modify. In the Modify BlueCat DNS/DHCP wizard, modify the parameter settings.

Note: If you modify any of the interface parameters or the name of the instance, the instance stops and restarts to put the changes into effect.

Updated: 2013-06-20

The SDX appliance collects statistics, such as the version of SDXTools running on the instance, of a BlueCat DNS/DHCP instance.

To view the statistics related to a BlueCat DNS/DHCP instance

1. Navigate to BlueCat DNS/DHCP > Instances.
2. In the details pane, click the arrow next to the name of the instance.

Updated: 2013-06-18

You can start, stop, restart, force stop, or force restart a BlueCat DNS/DHCP instance from the Management Service.

On the Configuration tab, expand BlueCat DNS/DHCP.

To start, stop, restart, force stop, or force restart a BlueCat DNS/DHCP instance

1. Click Instances.
2. In the details pane, select the instance on which you want to perform the operation, and then select one of the following options:
 - Start
 - Shut Down
 - Reboot
 - Force Shutdown
 - Force Reboot
3. In the Confirm message box, click Yes.

Updated: 2013-06-20

SDXTools, a daemon running on the third-party instance, is used for communication between the Management Service and the third-party instance.

Upgrading SDXTools involves uploading the file to the SDX appliance, and then upgrading SDXTools after selecting an instance. You can upload an SDXTools file from a client computer to the SDX appliance.

To upload an SDXTools file

1. In the navigation pane, expand Management Service, and then click SDXTools Files.
2. In the details pane, from the Action list, select Upload.
3. In the Upload SDXTools Files dialog box, click Browse, navigate to the folder that contains the file, and then double-click the file.
4. Click Upload.

To upgrade SDXTools

On the Configuration tab, expand BlueCat DNS/DHCP.

1. Click Instances.
2. In the details pane, select an instance.
3. From the Action list, select Upgrade SDXTools.
4. In the Upgrade SDXTools dialog box, select a file, click OK, and then click Close.

Updated: 2013-06-20

You can rediscover an instance to view the latest state and configuration of an instance. During rediscovery, the Management Service fetches the configuration. By default, the Management Service schedules instances for rediscovery of all instances once every 30 minutes.

On the Configuration tab, expand BlueCat DNS/DHCP.

1. Click Instances.
2. In the details pane, select the instance that you want to rediscover, and from the Action list, click Rediscover.
3. In the Confirm message box, click Yes.

CA Access Gateway

Jan 31, 2011

CA Access Gateway is a scalable, manageable, and extensible stand-alone server that provides a proxy-based solution for access control. CA Access Gateway employs a proxy engine that provides a network gateway for the enterprise and supports multiple session schemes that do not rely on traditional cookie-based technology.

The embedded web agent enables Single Sign-On (SSO) across an enterprise. CA Access Gateway provides access control for HTTP and HTTPS requests and cookieless SSO. Also, the product stores session information in the in-memory session store. Proxy rules define how the CA Access Gateway forwards or redirects requests to resources located on destination servers within the enterprise.

By providing a single gateway for network resources, CA Access Gateway separates the corporate network and centralizes access control.

Note: For more information about the features of CA Access Gateway, see the product documentation on [Wiki](#)

Updated: 2014-11-04

Before you can provision a CA Access Gateway instance, you must download an XVA image. After you have downloaded the XVA image, upload it to the NetScaler SDX appliance. Make sure you are using Management Service version 10.5 build 52.3.e or later on the NetScaler SDX appliance. To provision a CA Access Gateway, first you need to upload the XVA image to the SDX appliance and then provision an instance.

To upload an XVA image to the SDX appliance

1. On the **Configuration** tab, navigate to **CA Access Gateway > Software Images**.
2. In the details pane, under **XVA Files**, from the **Action** drop-down list, click **Upload**.
3. In the dialog box that appears, click **Browse**, and then select the XVA file that you want to upload.
4. Click **Upload**. The XVA file appears in the **XVA Files** pane.

To provision a CA Access Gateway instance

1. On the **Configuration** tab, navigate to **CA Access Gateway> Instances**.
2. In the details pane, click **Add**.
3. In the Provision CA Access Gateway wizard, follow the instructions on the screen.
4. Click **Finish**, and then click **Close**.

After you provision the instance, log on to the instance and perform the detailed configuration.

To modify the values of the parameters of a provisioned instance, in the details pane, select the instance that you want to modify, and then click **Modify**. In the Modify CA Access Gateway wizard, set the parameters to values suitable for your environment.

Note: If you modify any of the interface parameters or the name of the instance, the instance stops and restarts to put the change into effect.

Updated: 2014-11-04

The SDX appliance collects statistics, such as the version of SDXTools running on the instance, of a CA Access Gateway instance.

To view the statistics related to a CA Access Gateway instance

1. Navigate to CA Access Gateway > Instances.
2. In the details pane, click the arrow next to the name of the instance.

Updated: 2014-11-04

You can start, stop, restart, force stop, or force restart a CA Access Gateway instance from the Management Service.

On the Configuration tab, expand CA Access Gateway.

1. Navigate to CA Access Gateway > Instances.
2. In the details pane, select the instance on which you want to perform the operation, and then select one of the following options:
 - Start
 - Shut Down
 - Reboot
 - Force Shutdown
 - Force Reboot
3. In the Confirm message box, click Yes.

Palo Alto Networks VM-Series

Aug 31, 2015

Note: Provisioning Palo Alto VM-Series instances on a NetScaler SDX appliance is supported only on NetScaler release 10.1.e.

Palo Alto Networks VM-Series virtual firewalls use the same PAN-OS™ feature set that is available in the company's physical security appliances, providing all key network security functions. VM-Series on Citrix NetScaler SDX enables consolidation of advanced security and ADC capabilities on a single platform, for secure, reliable access to applications by businesses, business units, and service-provider customers. The combination of VM-Series on Citrix NetScaler SDX also provides a complete, validated, security and ADC solution for Citrix XenApp and XenDesktop deployments. You can provision, monitor, manage, and troubleshoot an instance from the Management Service.

Note: The total number of instances that you can provision on an SDX appliance depends on the NetScaler SDX hardware resources available .

Important: You must upgrade your XenServer version to version 6.1.0 and install the xs-netscaler-6.1.0-2.6.32.43 - 0.4.1.xs1.6.10.777.170770-100012 supplemental pack.

For more information about Palo Alto Network VM-Series, see [Palo Alto Network Documentation](#).

Before you can provision a Palo Alto VM-Series instance, you must download an XVA image from the Palo Alto Networks website, <https://support.paloaltonetworks.com/Updates/SoftwareUpdates/>. After you have downloaded the XVA image, upload it to the NetScaler SDX appliance. Make sure you are using Management Service version 10.1 build 120.130403.e or later on the NetScaler SDX appliance.

To upload an XVA image to the SDX appliance

1. On the **Configuration** tab, navigate to **PaloAlto VM-Series > Software Images**.
2. In the details pane, under **XVA Files**, from the **Action** drop-down list, click **Upload**.
3. In the dialog box that appears, click **Browse**, and then select the XVA file that you want to upload.
4. Click **Upload**. The XVA file appears in the **XVA Files** pane.

To provision a Palo Alto VM-Series instance

1. On the **Configuration** tab, navigate to **PaloAlto VM-Series > Instances**.
2. In the details pane, click **Add**.
3. In the Provision PaloAlto VM-Series wizard, follow the instructions on the screen.
4. Click **Finish**, and then click **Close**.

After you provision the instance, log on to the instance and perform the detailed configuration.

To modify the values of the parameters of a provisioned instance, in the details pane, select the instance that you want to modify, and then click **Modify**. In the Modify PaloAlto VM-Series wizard, set the parameters to values suitable for your environment.

Note: If you modify any of the interface parameters or the name of the instance, the instance stops and restarts to put the change into effect.

The SDX appliance collects statistics, such as the version of SDXTools running on the instance, of a Palo Alto VM-Series

instance.

To view the statistics related to a Palo Alto VM-Series instance

1. Navigate to PaloAlto VM-Series > Instances.
2. In the details pane, click the arrow next to the name of the instance.

You can start, stop, restart, force stop, or force restart a PaloAlto VM-Series instance from the Management Service.

On the Configuration tab, expand PaloAlto VM-Series.

1. Navigate to PaloAlto VM-Series > Instances.
2. In the details pane, select the instance on which you want to perform the operation, and then select one of the following options:
 - Start
 - Shut Down
 - Reboot
 - Force Shutdown
 - Force Reboot
3. In the Confirm message box, click Yes.

You can ping a PaloAlto VM-Series instance from the Management Service to check whether the device is reachable. You can trace the route of a packet from the Management Service to an instance to determine the number of hops involved in reaching the instance.

You can rediscover an instance to view the latest state and configuration of an instance. During rediscovery, the Management Service fetches the configuration and the version of the PaloAlto VM-Series running on the SDX appliance. By default, the Management Service schedules instances for rediscovery once every 30 minutes.

On the Configuration tab, expand PaloAlto VM-Series.

To Ping an instance

1. Click **Instances**.
2. In the details pane, select the instance that you want to ping, and from the Action list, click **Ping**. The Ping message box shows whether the ping is successful.

To Trace the route an instance

1. Click **Instances**.
2. In the details pane, select the instance that you want to ping, and from the Action list, click **TraceRoute**. The **Traceroute** message box displays the route to the instance.

To rediscover an instance

1. Click **Instances**.
2. In the details pane, select the instance that you want to rediscover, and from the Action list, click **Rediscover**.
3. In the Confirm message box, click **Yes**.

NITRO API

Jun 03, 2014

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 relevant libraries that are packaged as separate Software Development Kits (SDKs).

Note: You must have a basic understanding of the NetScaler SDX appliance before using NITRO. 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 above version 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 where .NET framework 3.5 or above version is available. The .NET framework can be downloaded from <http://www.microsoft.com/downloads/en/default.aspx>.

Obtaining the NITRO Package

Jun 03, 2014

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 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:

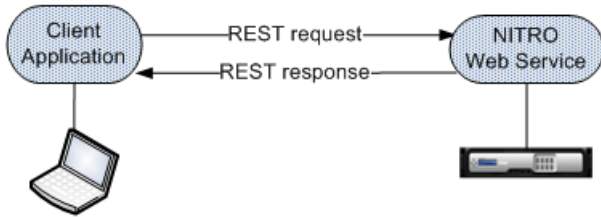
- The REST package contains only documentation for using the REST interfaces.

How NITRO Works

Jun 03, 2014

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 the 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 the 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

Jan 28, 2011

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.

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();
```

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);
```

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

Jan 28, 2011

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.

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();
```

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);
```

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

Jan 28, 2011

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.

Updated: 2014-06-11

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: You must use the session ID in all further NITRO operations on the appliance.

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. For example, to modify the timeout period to 60 minutes, the request payload is:

object=

```
{
  "login":
  {
    "username":"nsroot",
    "password":"verysecret",
    "timeout":3600
  }
}
```

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...

Updated: 2014-06-11

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

Each NetScaler SDX resource has an 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>`.

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 vpx1:

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


```

"ns":
{
  "name":"vpx1",
  "ip_address":"192.168.100.2",
  "netmask":"255.255.255.0",
  "gateway":"192.168.100.1",
  "image_name":"nsvpx-9.3-45_nc.xva",
  "vm_memory_total":2048,
  "throughput":1000,
  "pps":1000000,
  "license":"Standard",
  "profile_name":"ns_nsroot_profile",
  "username":"admin",
  "password":"admin",

  "network_interfaces":
  [
    {
      "port_name":"10/1"
    },
    {
      "port_name":"10/2"
    }
  ]
}
}

```

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 and continue if one command fails:

- **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 and continue if one command fails:

- **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"
 }
]
}

```

Updated: 2014-06-11

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"
}
```