SDX 11.0

Apr 19, 2016

REST Web Services

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 8005/8010/8015/8200/8400/8600/8800 Appliance to a NetScaler SDX 8010/8015/8400/8600 Appliance

Converting a NetScaler MPX 24100 and 24150 Appliance to a NetScaler SDX 24100 and 24150 Appliance

SDX Command Reference

System

NetScaler

XenServer

Introduction

Sep 01, 2016

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

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

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

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.

SDX 11.0 adds support for the following:

- Single Bundle Upgrade
- Simplified Backup and Restore
- Password less authentication for accessing SDX command line interface
- Visualizer
- Syslog viewer
- First time user wizard
- Support for SNMP v3 traps
- Support for TLS 1.0, 1.1, and 1.2

SDX 11.0 also provides many usability enhancements.

For detailed information about SDX 11.0 enhancements, known issues, and bug fixes, see: About the NetScaler 11.0 Release.

NetScaler SDX Hardware and Component Compatibility Matrix

Dec 31, 2017

See NetScaler SDX Hardware-Software Compatibility Matrix.

Hardware Installation

Jun 28, 2017

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.

> ## Note
>
> For information about configuring the Citrix NetScaler SDX 14030/14060/14080 FIPS appliance, see Configuring an SDX 14000 FIPS Appliance.

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).

This document includes the following details:

- LCD Display and LED Status Indicators
- Ports

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	No link.
			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 green	Traffic is passing through the port.
Management (RJ45)	Left	Speed	Off	No connection, or a traffic rate of 10 megabits per second (Mbps).
			Green	Traffic rate of 100 Mbps.

Port Type	LED Location	LED Function	LED Color	LED Indicates
			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 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,	Citrix NetScaler 1G SFP Ethernet Copper	n/a	Category 5 (Cat-5) Copper Cable	100 m	SDX 8015/8400/8600, SDX 22040/22060/22080/22100/22120, SDX 24100/24150

EW3E0000235, EW3F0000235, EW3P0000143, EW3X0000235, EW3Z0000087	(100m) - **4 Pack**				

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,	Citrix NetScaler 1G SFP Ethernet Short Range (300m) -	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	550 m	

EW3P0000557, EW3X0000710, EW3Z0000585	Single		MMF, 500MHz-km (OM2)		
			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,	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

EW3X0000711, EW3Z0000586					

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 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-km	26 m	

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,	Citrix NetScaler 10G SFP+ Ethernet Long Range	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 17550/19550/20550/21550, SDX

EW3F0000711, EW3P0000558, EW3X0000711, EW3Z0000586	(10km) - **Single**				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.
This document includes the following details:

- Power Supply
- Solid-State Drive
- Hard Disk Drive
- Direct Attach Cable

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

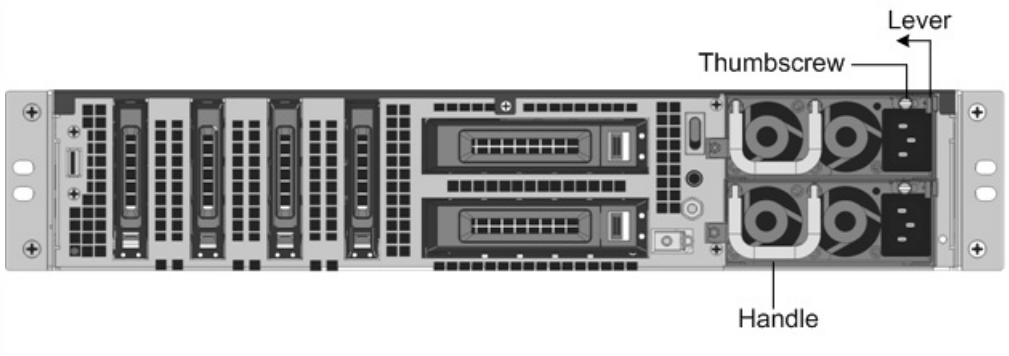
Citrix NetScaler SDX platforms can accommodate two power supplies, except the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 platforms which can accommodate four power supplies. All NetScaler appliances function properly with a single power supply, except the SDX 22040/22060/22080/22100/22120 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.

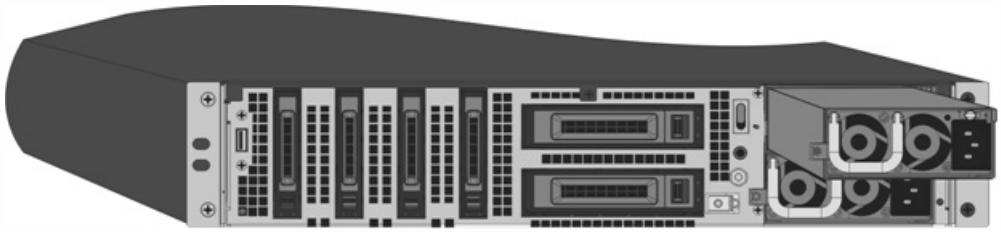
If the appliance has two power supplies, you can replace one power supply without shutting down the appliance, provided the other power supply is working.

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

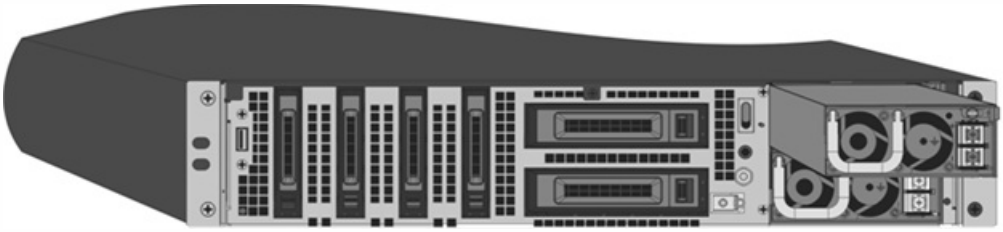
Citrix NetScaler SDX platforms can accommodate two power supplies, except the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 platforms which can accommodate four power supplies. All NetScaler appliances function properly with a single power supply, except the SDX 22040/22060/22080/22100/22120 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.

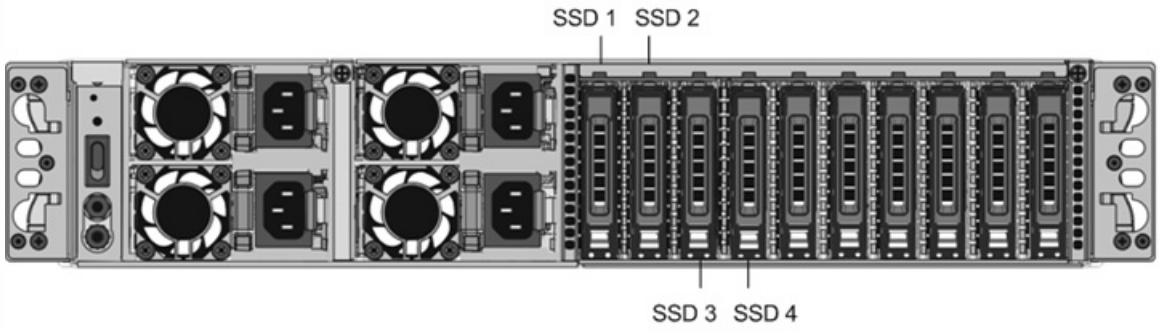
A solid-state drive (SSD) is a high-performance device that stores data in solid-state flash memory.

Replacing a Solid-State Drive

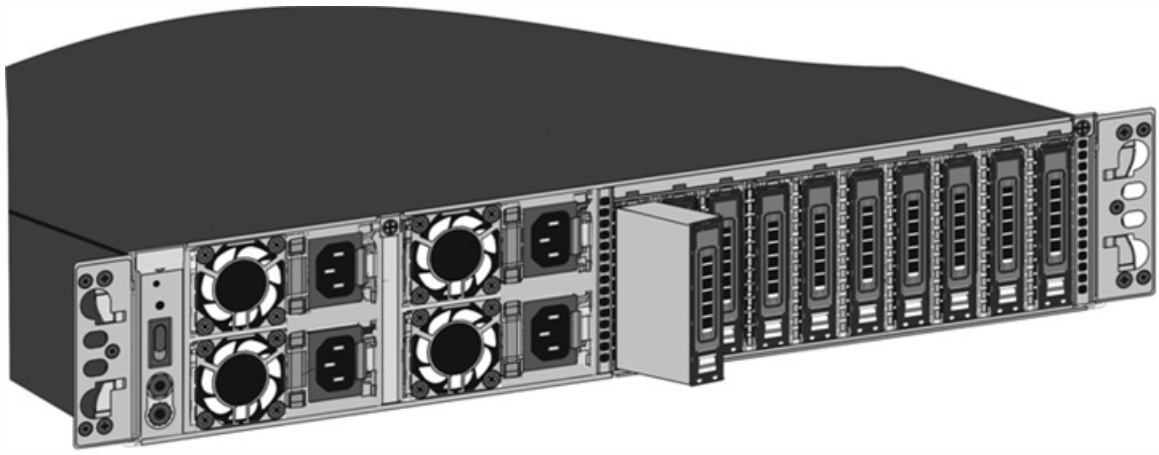
To replace a solid-state drive on SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 appliances

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

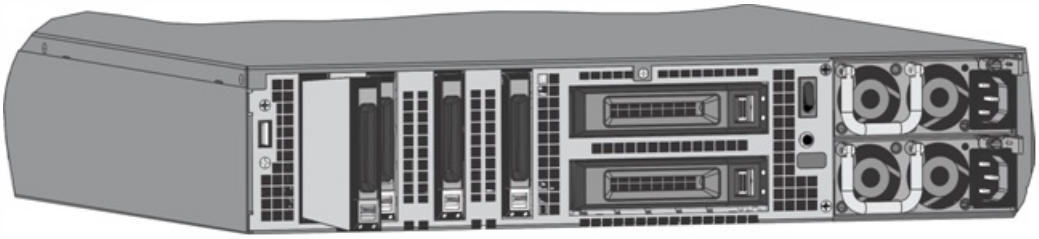
Replacement solid-state drives (SSDs) contain a pre-installed version of the NetScaler software and a generic configuration file (ns.conf), but they do not contain SSL-related certificates and keys, or custom boot settings. After installing the replacement SSD, you have to restore the configuration files 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 Shutdown 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.

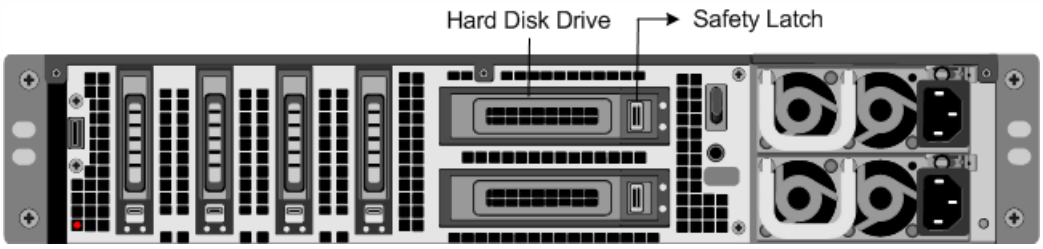
A hard disk drive (HDD) stores logs and other data files. Files stored on the HDD include the newnslog files, dmesg and messages files, and any core/crash files. The HDD comes in various capacities, depending on the Citrix NetScaler platform. Hard drives are used for storing files required at runtime.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

Replacing a Hard Disk Drive

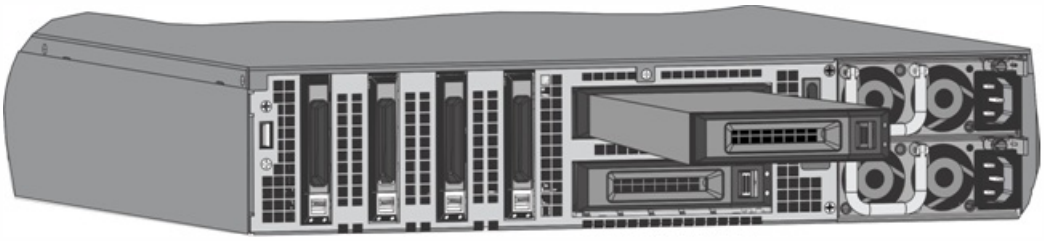
A hard disk drive (HDD) stores log files and other user files. Collection of new log files begins upon boot-up with the new HDD. Product documentation can be downloaded from "MyCitrix.com" and reinstalled to the /var/netscaler/doc location.

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.

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:

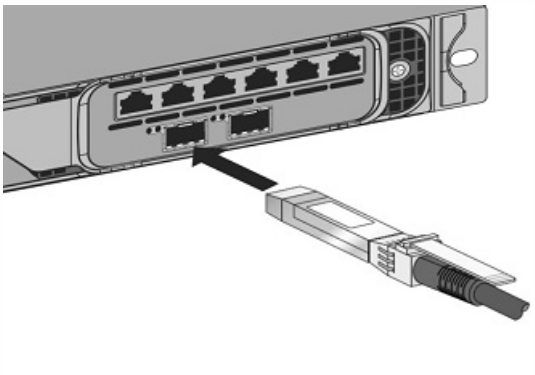
- DAC is supported only on 10G ports. Do not insert a DAC into a 1G port.
- Do not attempt to unplug the integrated copper cable from the transceiver and insert a fiber cable into the transceiver.

Installing a Direct Attach Cable

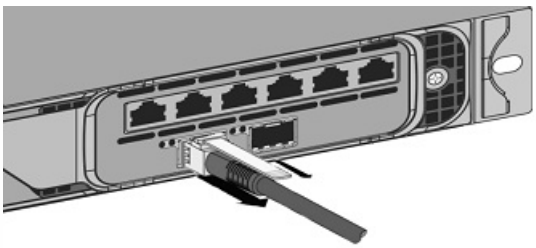
Note: The illustrations in the following figures are only for reference and might not represent the actual NetScaler appliance.

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

Dec 19, 2016

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

Citrix NetScaler SDX 8015, SDX 8400, and SDX 8600

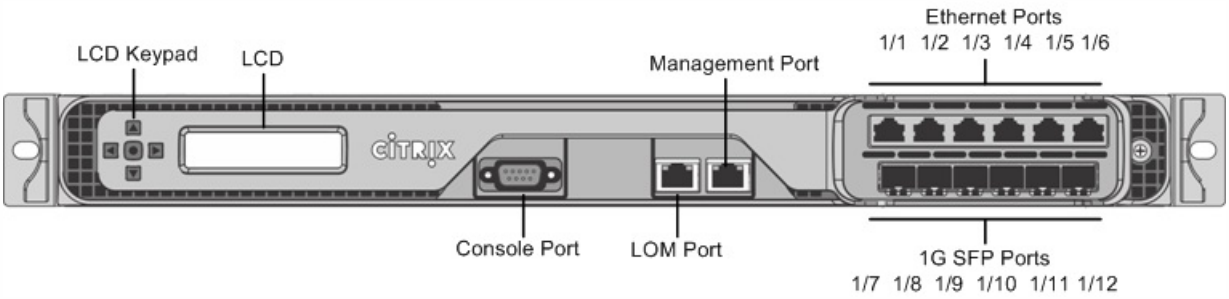
Aug 01, 2017

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+)

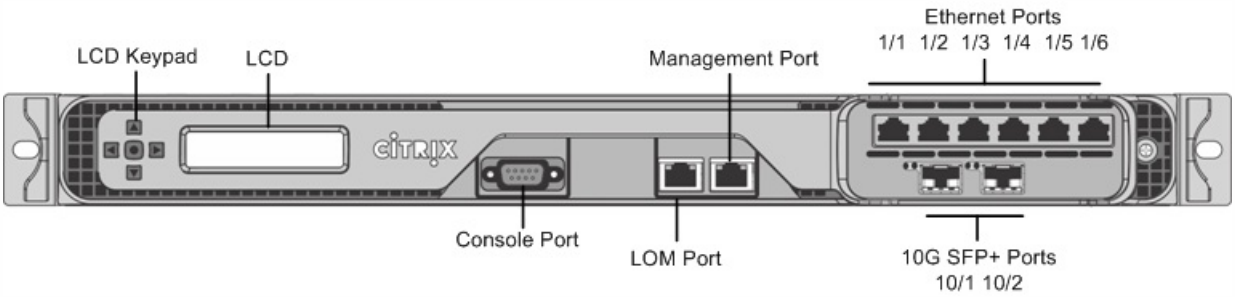
The following figure shows the front panel of the SDX 8015/8400/8600 (6x10/100/1000Base-T copper Ethernet ports + 6x1G SFP) appliance.

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:

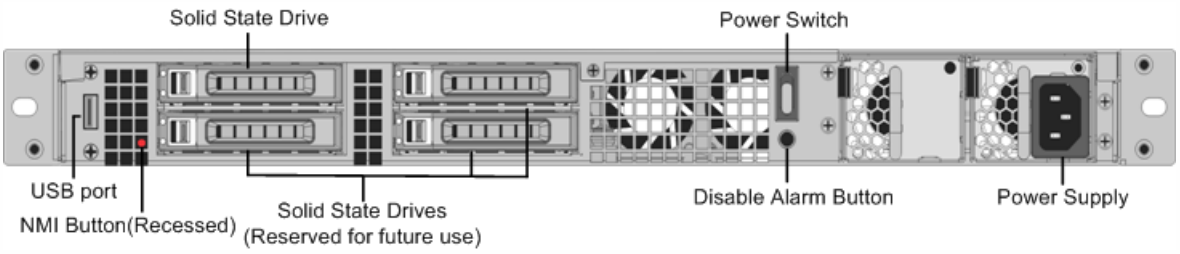
- RS232 serial console port.
- One 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the NetScaler software.
- One 10/100/1000Base-T copper Ethernet management port (RJ45), numbered 0/1. The management port 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:

- 300 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.

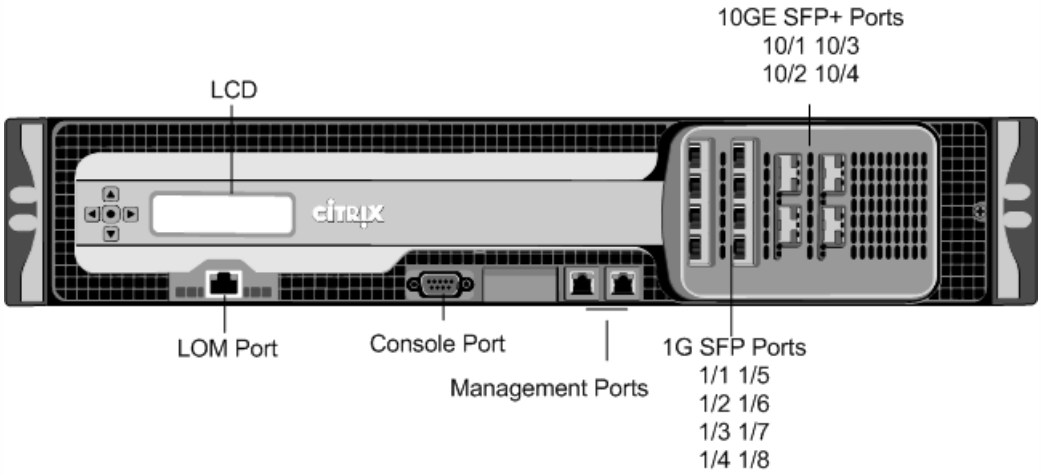
Citrix NetScaler SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500, and SDX 20500

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

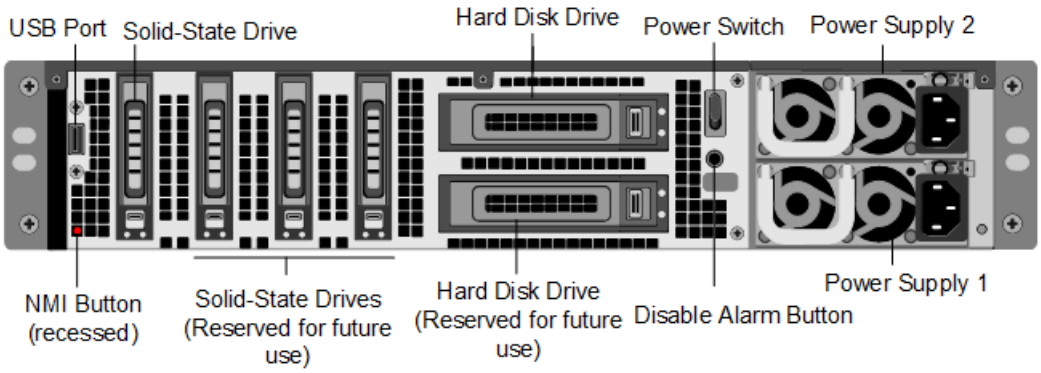


The SDX 11500/13500/14500/16500/18500/20500 appliances have the following ports:

- 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:

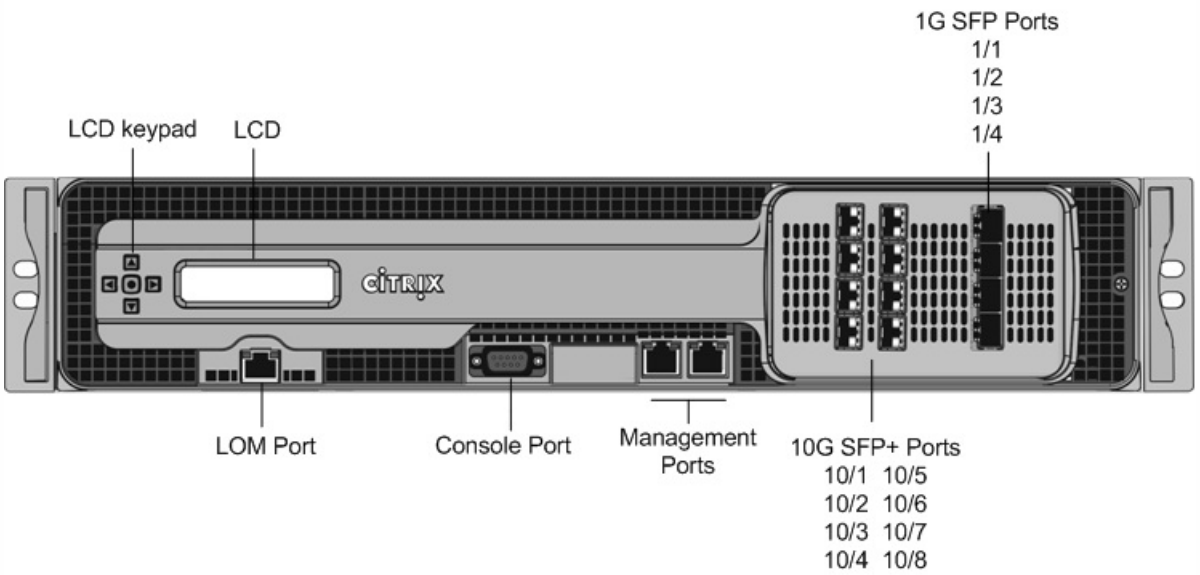
- 160 GB removable solid-state drive that is used to store the NetScaler software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Non-maskable 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

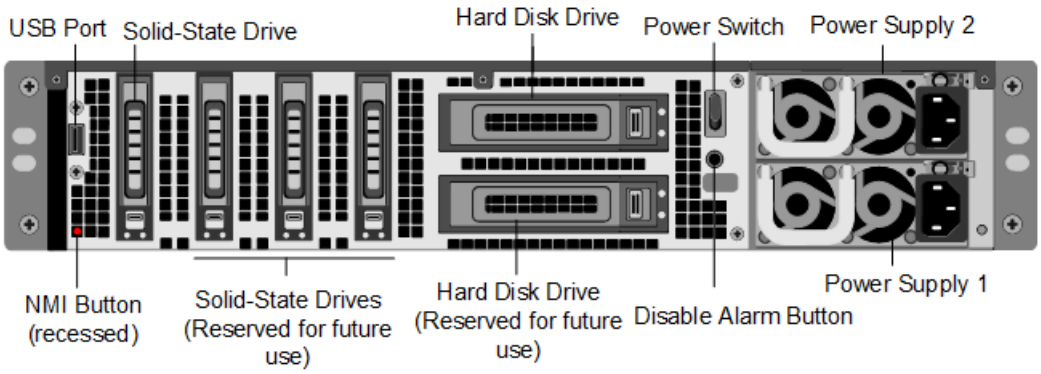


The SDX 11515/11520/11530/11540/11542 appliances have the following ports:

- 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 2. 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.

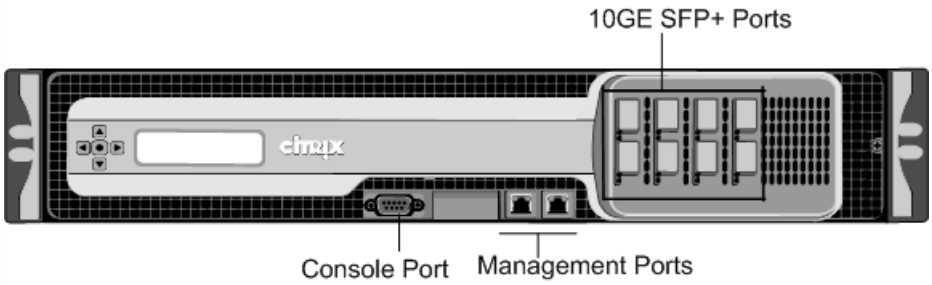
Citrix NetScaler SDX 17500, SDX 19500, and SDX 21500

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

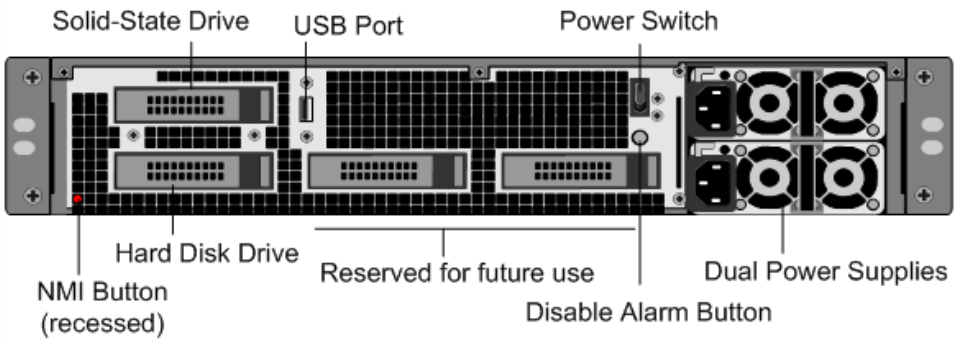


The SDX 17500/19500/21500 appliances have the following ports:

- 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.

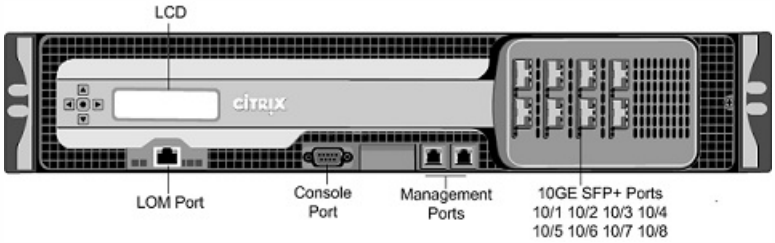
Citrix NetScaler SDX 17550, SDX 19550, SDX 20550, and SDX 21550

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

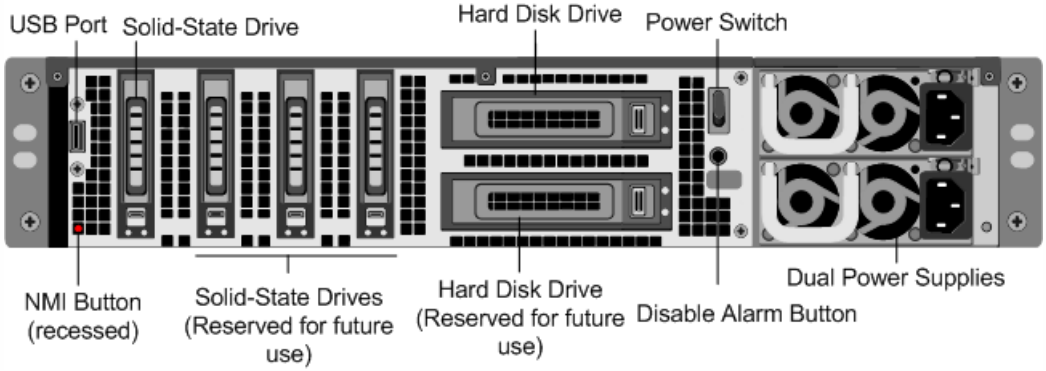


The SDX 17550/19550/20550/21550 appliance has the following ports:

- 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

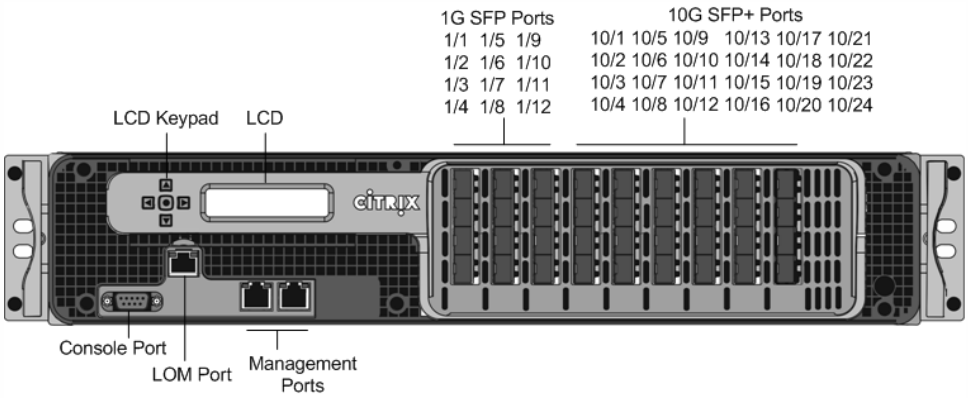
Oct 25, 2013

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+)

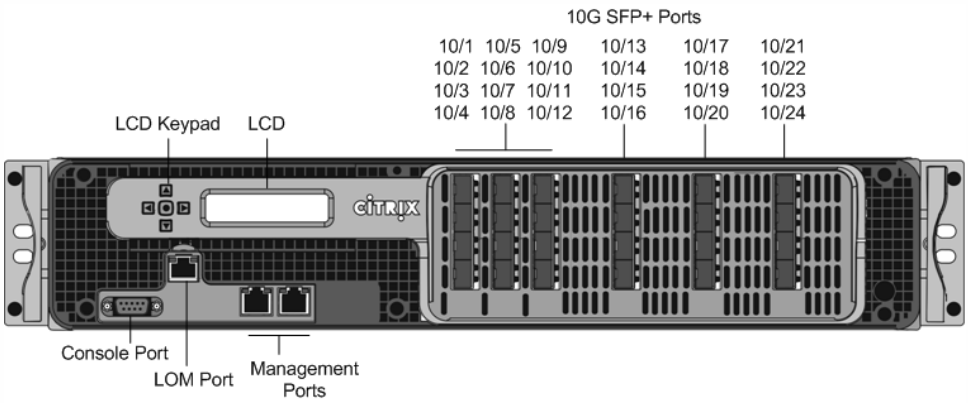
The following figure shows the front panel of the SDX 22040/22060/22080/22100/22120 (12x1G SFP + 24x10G SFP+) appliance.

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

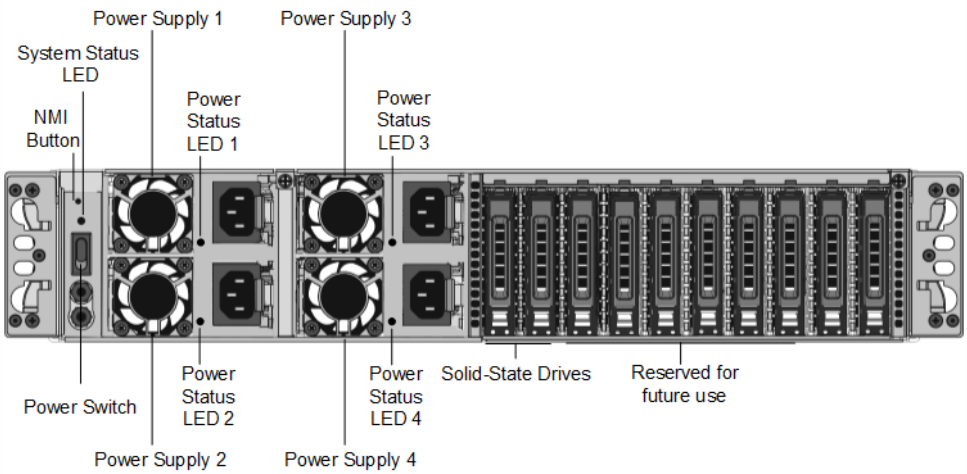


Depending on the model, the appliance has the following ports:

- 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 LCD Display and LED Status Indicators.

  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 LCD Display and LED Status Indicators.
- 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.

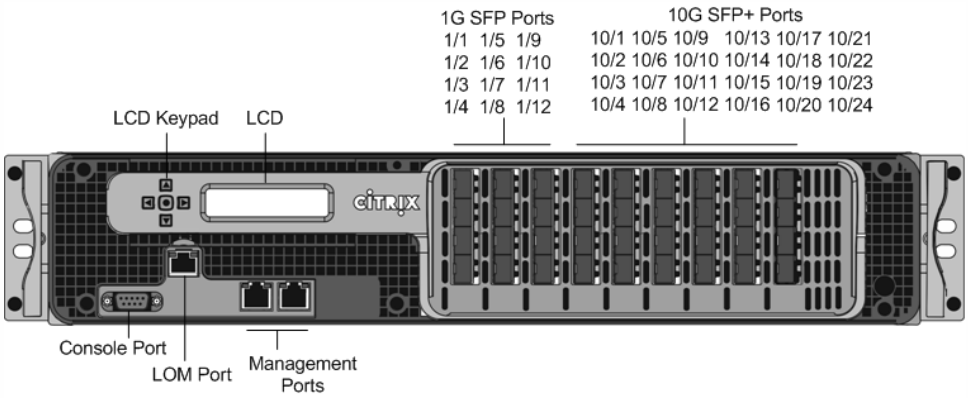
Citrix NetScaler SDX 24100 and SDX 24150

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

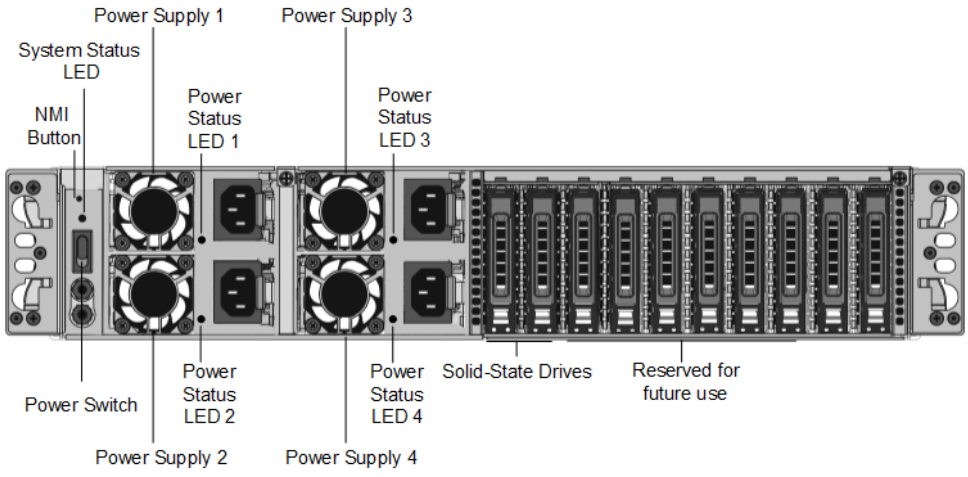


Depending on the model, the appliance has the following ports:

- 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 LCD Display and LED Status Indicators.

  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 LCD Display and LED Status Indicators.
- 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

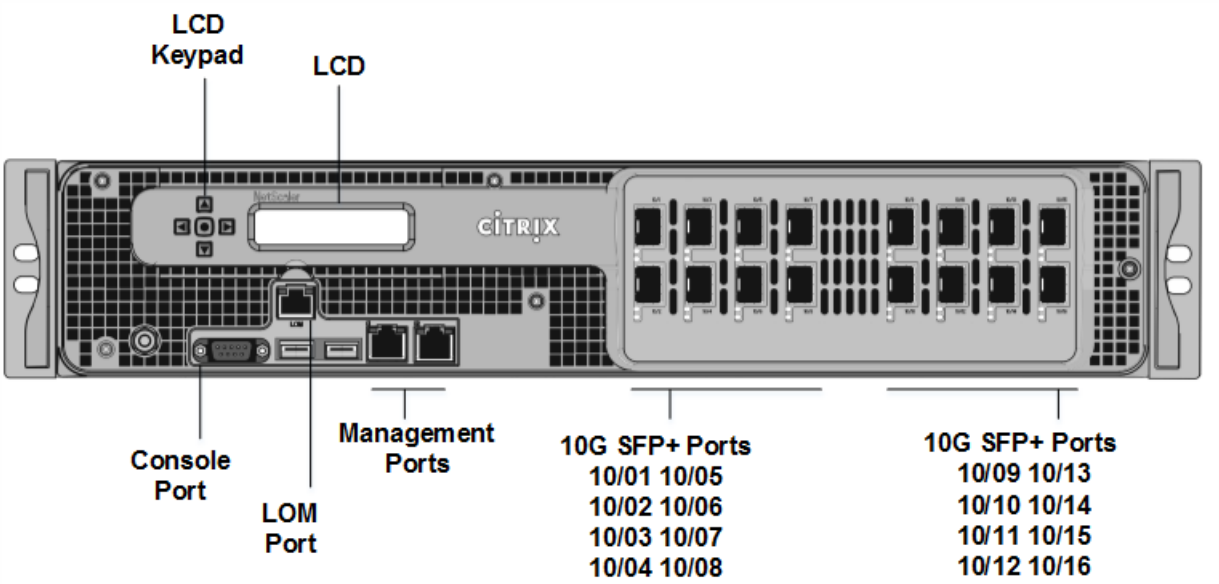
Dec 22, 2016

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+).

Note: For information about NetScaler SDX hardware and component compatibility matrix, see https://docs.citrix.com/en-us/sdx/11/sdx-ag-supported-versions-ref.html.

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



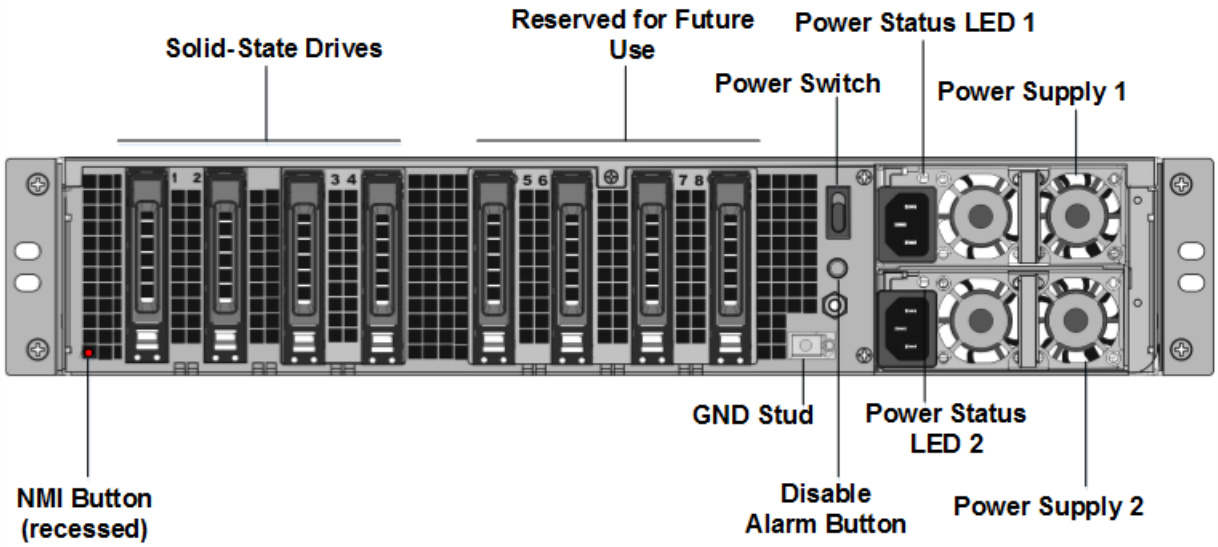
The NetScaler SDX 14020/14030/14040/14060/14080/14100 appliances have the following ports:

- 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

May 11, 2017

The following tables summarize the specifications of the hardware platforms. The latest NetScaler datasheet is available at https://www.citrix.com/products/netscaler-adc/.

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	**6x1G SFP + 6x10/100/1000Base-T copper Ethernet model**: 6xcopper/fiber 1G SFP ports, 6x10/100/1000Base-T copper Ethernet ports **2x10G SFP+ 6x10/100/1000Base-T copper Ethernet model**: 6xcopper/fiber 1G SFP ports,	8x1G SFP ports	**8x1G SFP + 4x10G SFP+ model**: 8xcopper/fiber 1G SFP ports **8x1G SFP + 8x10/100/1000Base-T copper Ethernet model**: 8xcopper/fiber 1G SFP ports, 8x10/100/1000Base-T copper Ethernet ports
Ports - 10G	**2x10G SFP+ 6x10/100/1000Base-T copper Ethernet model**: 2x10G SFP+ Ports	4x10G SFP+ ports	**8x1G SFP + 4x10G SFP+ model**: 4x10G SFP+ ports
Number of Power Supplies	1	2	2

Maximum NetScaler Instances 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
	SDX 8015/SDX 8400/SDX 8600	SDX 11500/SDX 13500/SDX 14500/SDX 16500/SDX 18500/SDX 20500	SDX 11515/11520/11530/11540/11542

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	**12x1G SFP + 24x10G SFP+ model**: 100-240VAC

	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
			6.0-12.0A **24100/SDX 22120 model:** 100-240VAC 50/60Hz 6.5-15.5A	50/60Hz 6.0-12.0A
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	28¼ in or 72 cm	28¼ 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 Class A), CE, C-Tick, VCCI-A	FCC (Part 15 Class A), CE, C-Tick, VCCI-A	FCC (Part 15 Class A), CE (EN55022/55024), C-Tick, VCCI	FCC (Part 15 Class A), CE (EN55022/55024), C-Tick, VCCI
Compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE

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.

This document includes the following details:

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

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.

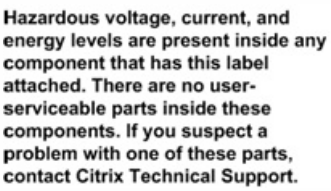
Note: You can order the following rail kits separately.

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

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:



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.

This document includes the following details:

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 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

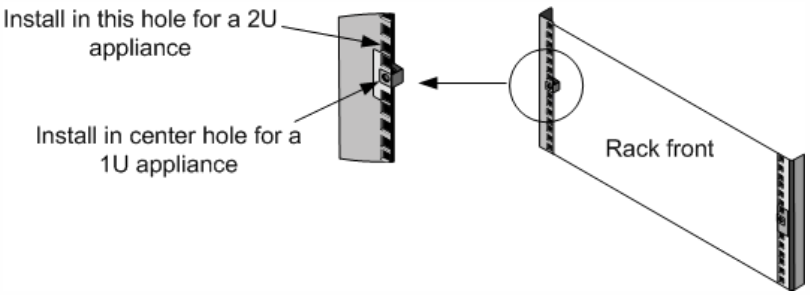
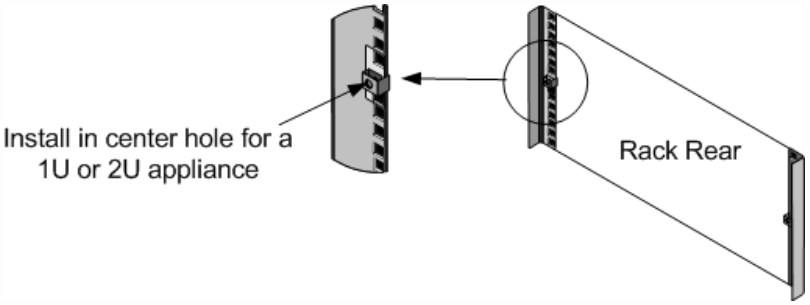
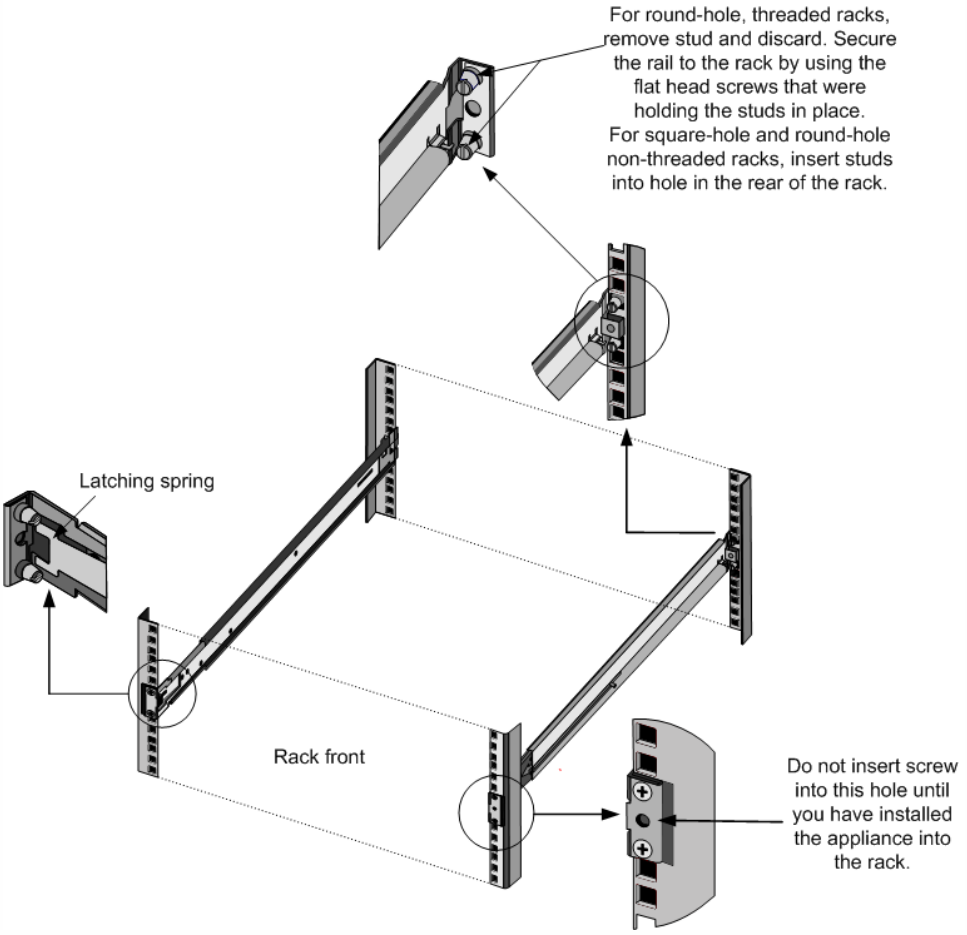


Figure 3. Installing Retainers into the Rear Rack Posts



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.

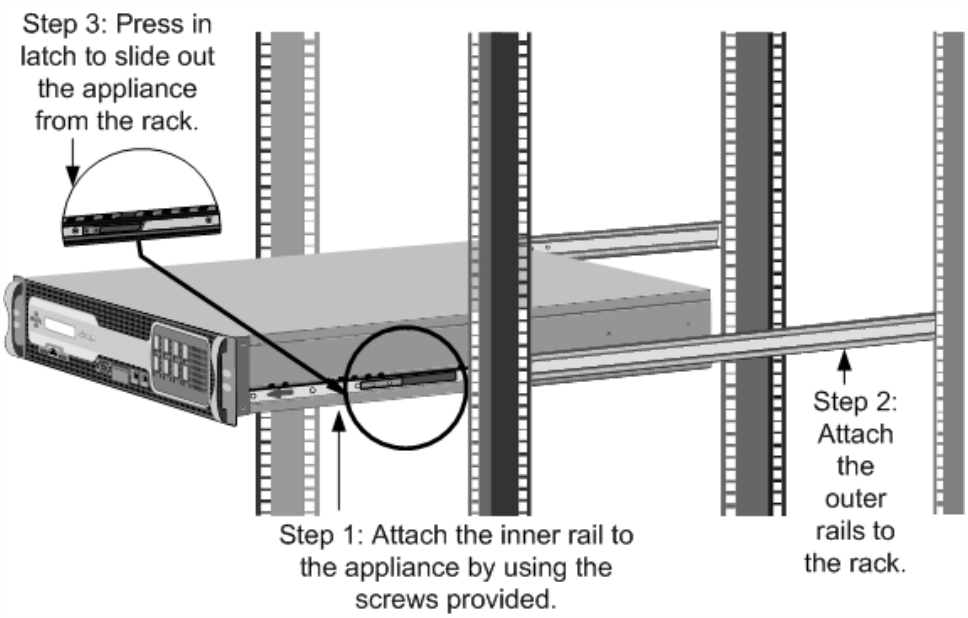
   Figure 4. Installing the Rail Assembly to the Rack



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



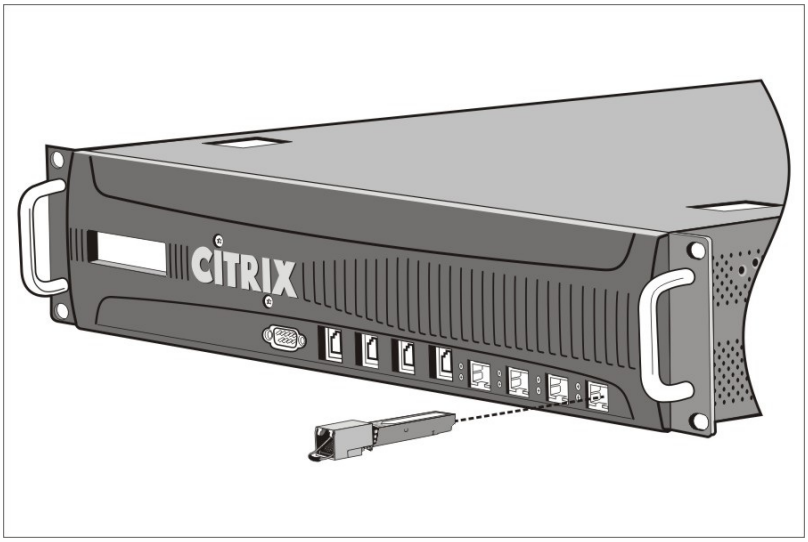
Note: This section applies to the SDX 8015/8400/8600, SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, SDX 22040/22060/22080/22100/22120, and SDX 24100/24150 appliances.
A Small Form-Factor Pluggable (SFP) is a compact transceiver that can operate at speeds of up to 1 gigabit 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.

Note: This section applies to the SDX 8015/8400/8600, SDX 11500/13500/14500/16500/18500/20500, SDX 11515/11520/11530/11540/11542, 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.

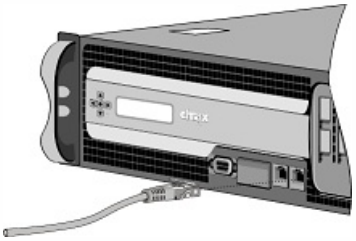
When the appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

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.

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.

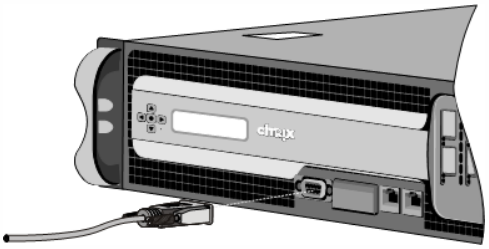
3. Verify that the LED glows amber when the connection is established.

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.

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.

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.

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

May 11, 2017

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, click here.

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.

This document includes the following details:

- Initial Configuration through the Management Service User Interface
- Initial Configuration through the Serial Console
- Changing the Password of the Default User Account

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.

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.
   - 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.

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	2.52/3.02/3.33/3.39	3.39	9.3_65.x, 10.1_123.x, 10.5

Hardware	Ships With Version	Recommended Version	Minimum NetScaler Version to avoid PS failure issues
SDX 17550/19550/20550/21550	2.63/3.22/3.30	3.22	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.

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.

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

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 theNetScaler 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.

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.

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 in 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 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.

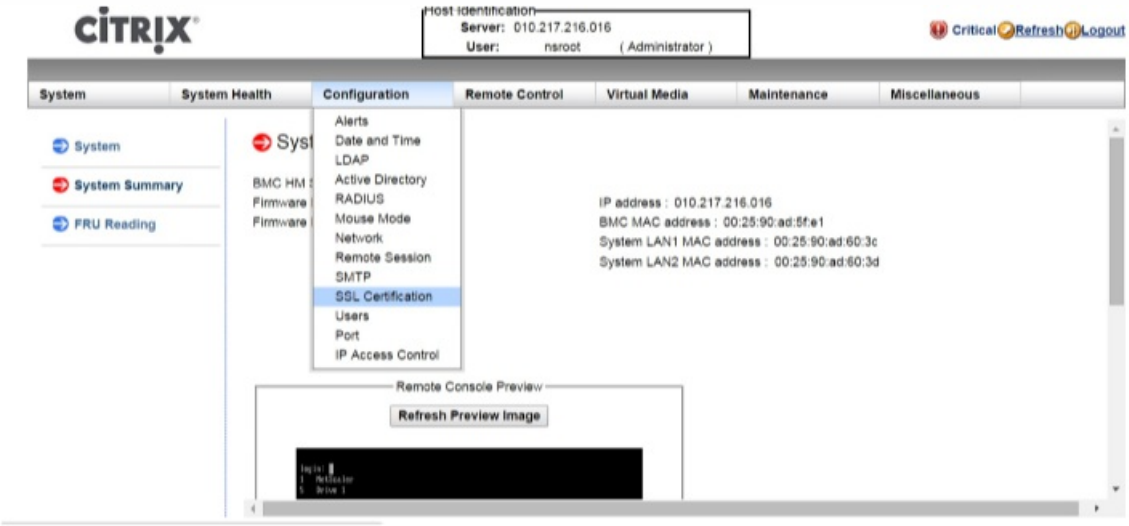
To encrypt SNMP alerts, setup an SSL certificate and private key. In the GUI, navigate to **Configuration** > **SSL Certification** and apply the SSL certificate and private key. See the NetScaler Secure Deployment Guide for more information about how to securely deploy the LOM in your network. To enable 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:

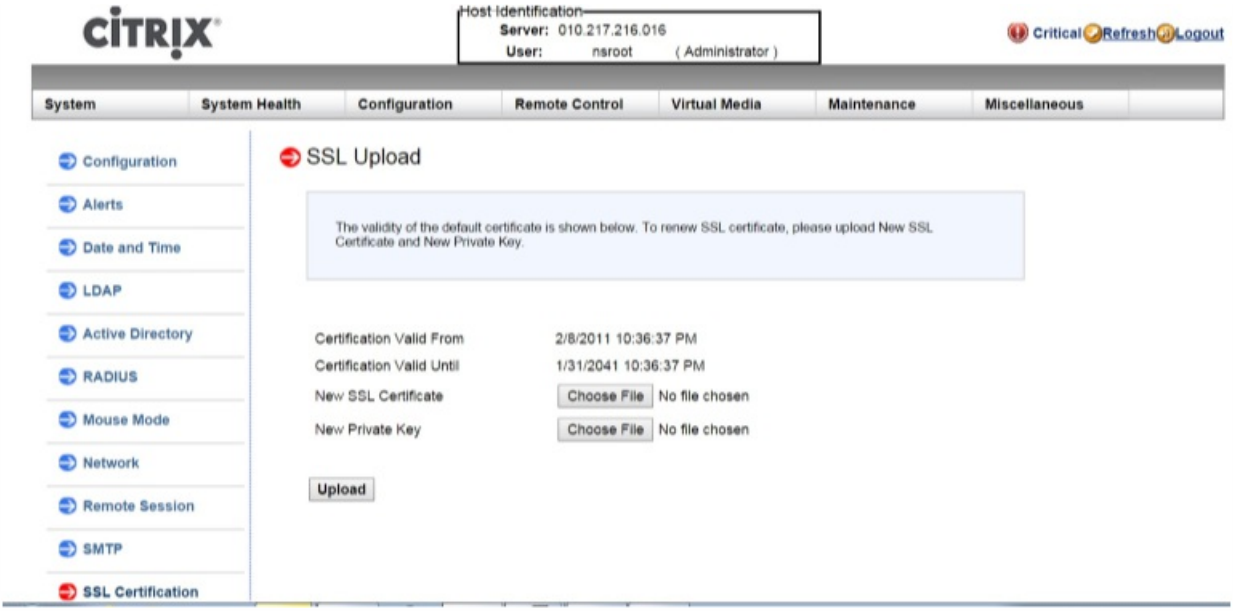
ipmitool raw 0x30 0x41 0x1

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.

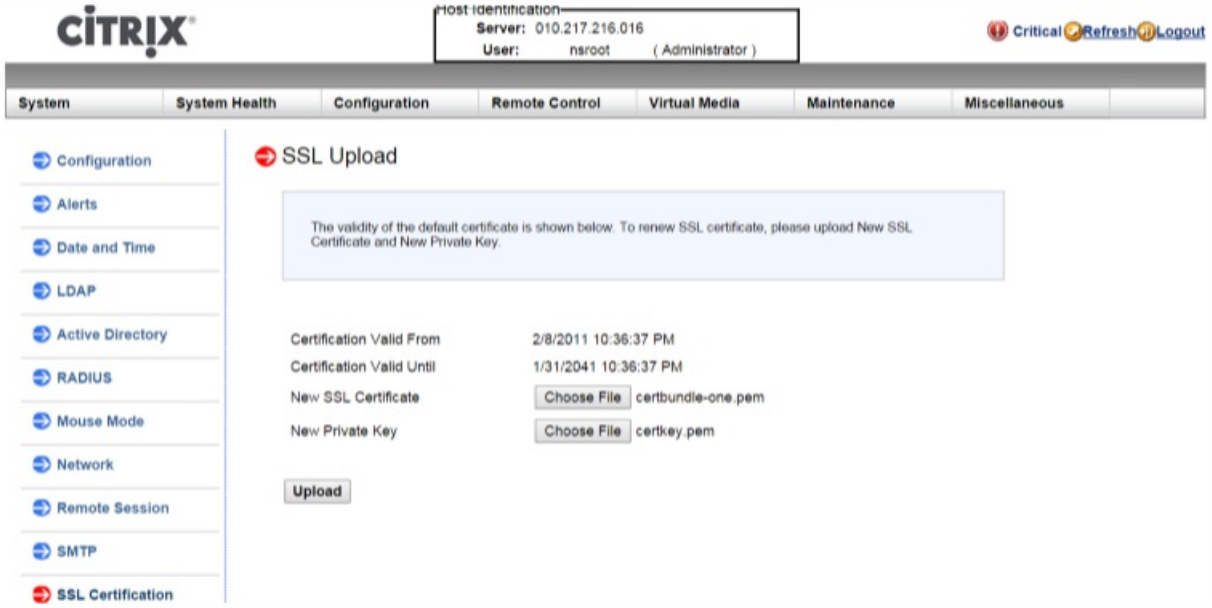
1. Navigate to Configuration > SSL Certification.



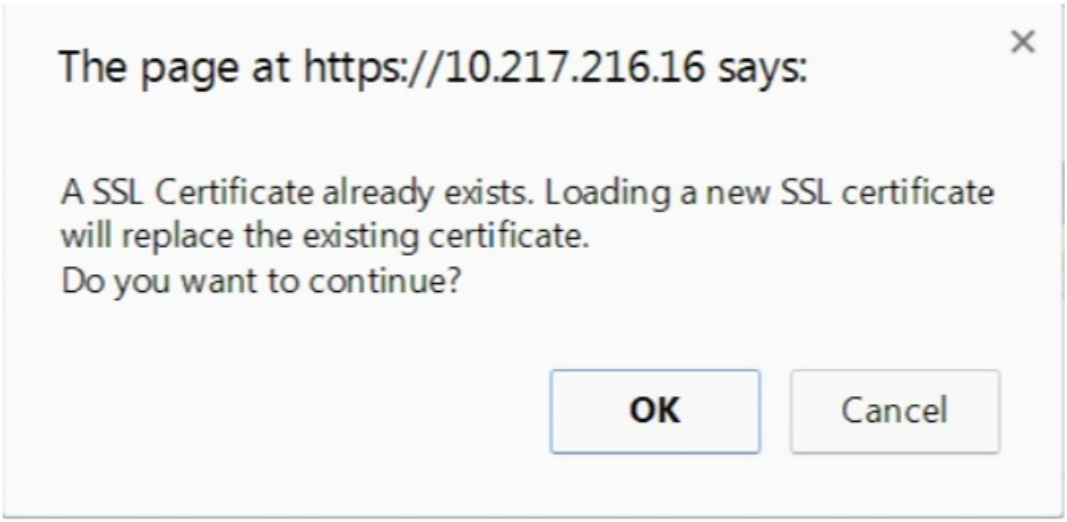
2. In the right pane, click the Choose File buttons to select a new SSL certificate and a new private key.



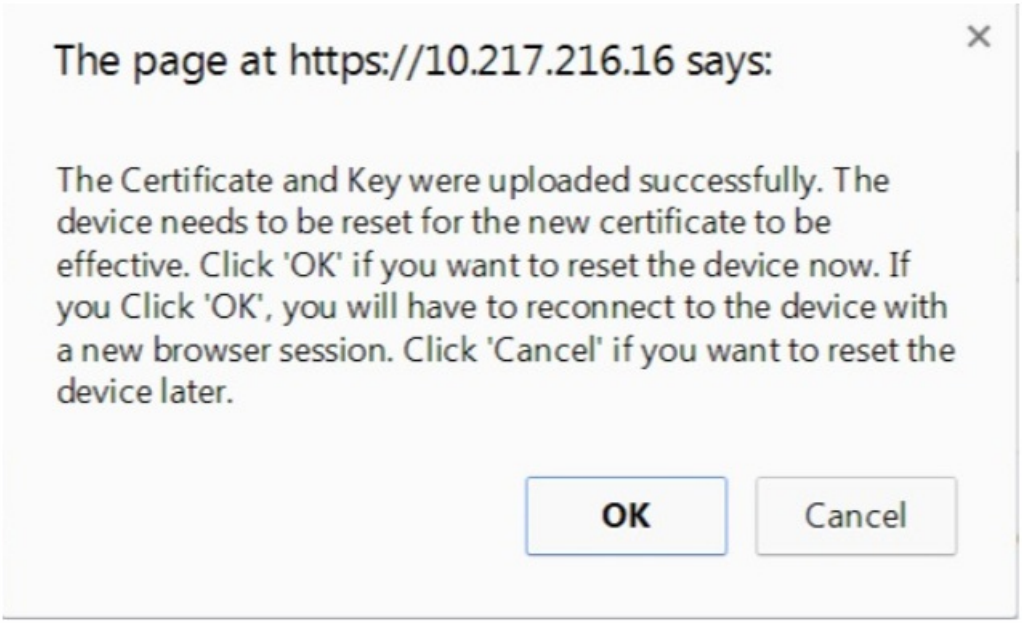
3. To verify that you have selected the correct certificate and private key, check the file names of the certificate and key, which appear next to the Choose File buttons.



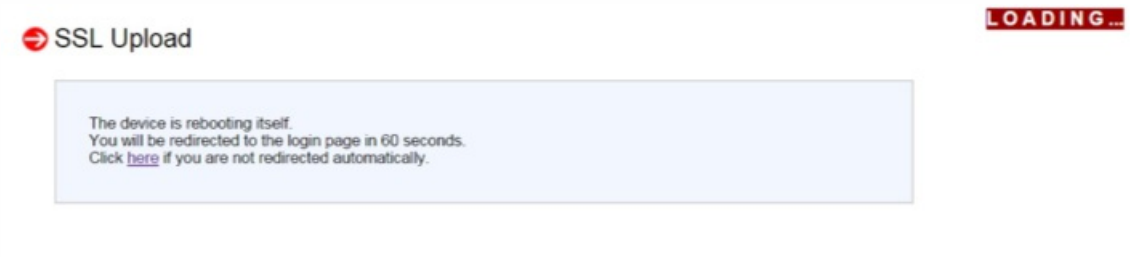
4. Click Upload. A message informs you that uploading a new SSL certificate replaces the existing (default) certificate.
5. Click OK.



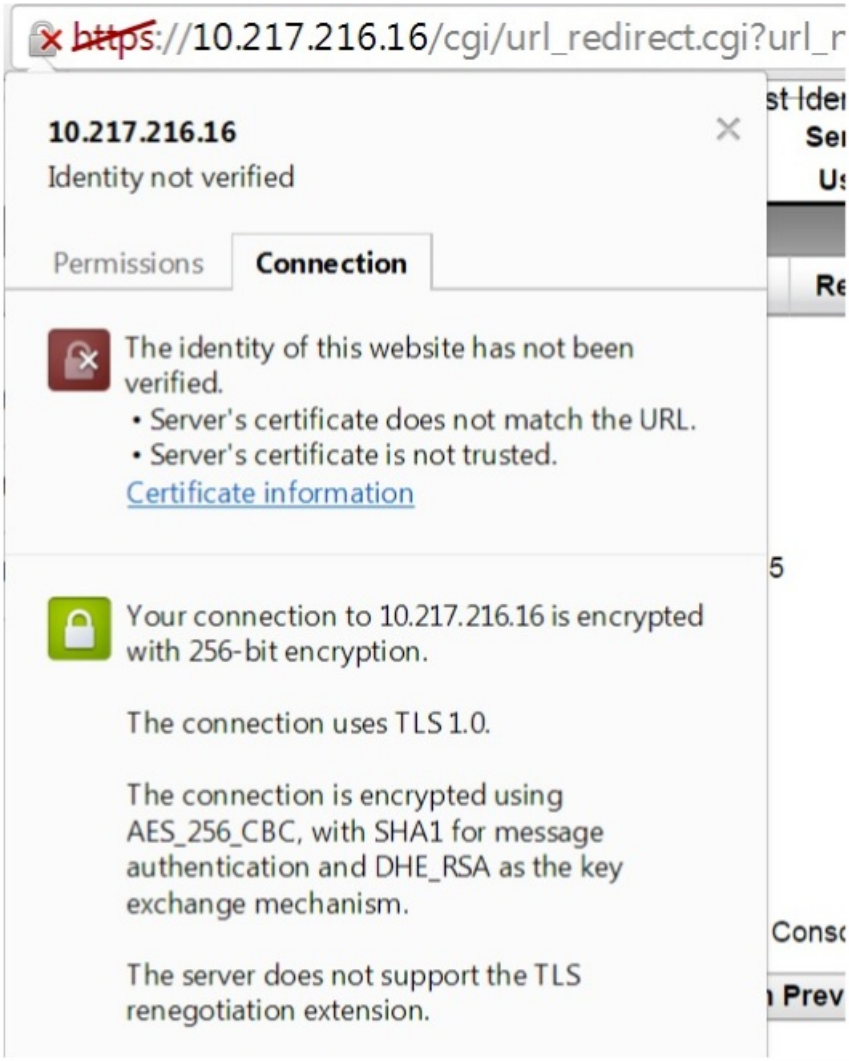
6. When a message informs you that the certificate and key have been uploaded successfully, click OK to reset the device.



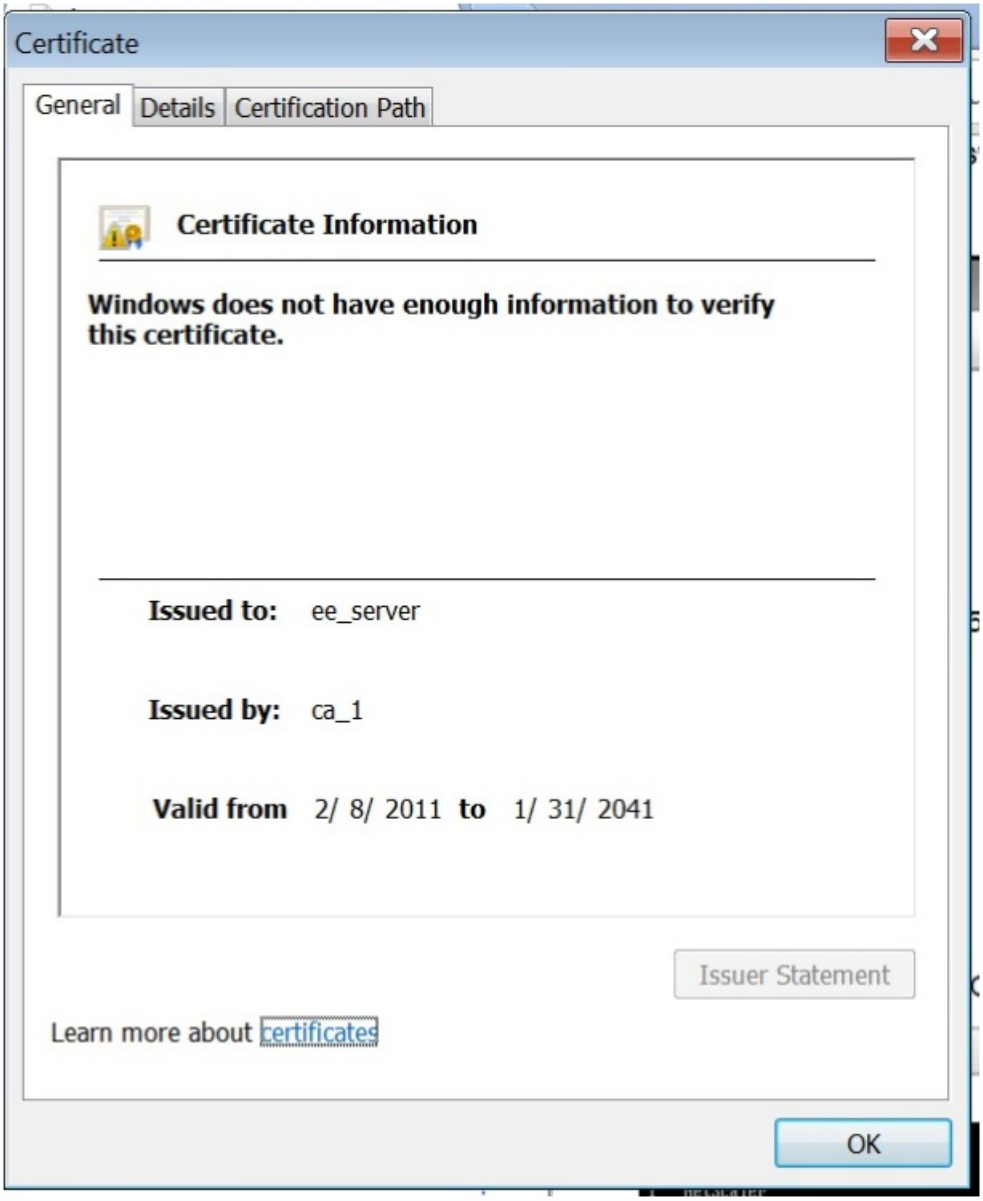
The reset takes approximately 60 seconds. You are then redirected to the logon page.



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.

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.

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
Gratituous 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.

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.

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.

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

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.

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

At the shell prompt, type:

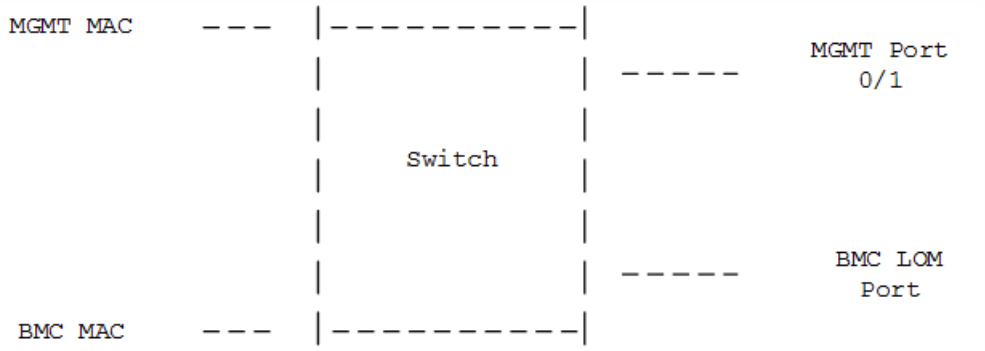
ipmitool raw 0x30 0x41 0x1

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.

Navigate to Miscellaneous > BIOS Post Snooping.

At the prompt, type:

ipmitool raw 0x30 0x2a

Getting Started with the Management Service User Interface

May 04, 2017

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.

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.

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.

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.

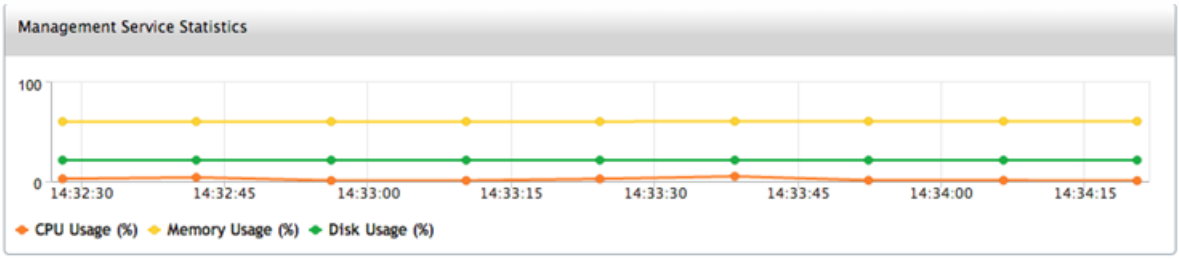
You can access the console of NetScaler instances, the Management Service, XenServer, and third party VMs from the Management Service interface. This is particularly helpful in debugging and troubleshooting the instances hosted on the NetScaler SDX appliance.

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.

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



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.

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.

Single Bundle Upgrade

May 15, 2018

For 10.5 and previous releases, the NetScaler SDX appliance setup includes setting up XenServer hypervisor, its supplemental packs and hotfixes, the Management Service, and NetScaler virtual machines. Each of these components has a different release cycle. Therefore, updating each component independently, as allowed by NetScaler SDX 10.5 and earlier releases, makes maintenance difficult. Updating each component separately also leads to unsupported combinations of components.

The single bundle image upgrade is available from 11.0 and later releases. The single bundle image combines all the components including the Management Service in a single image file called the NetScaler SDX image. The NetScaler instance (VPX) image is a separate image and is not included in the NetScaler SDX single bundle image.

By using the NetScaler SDX image, you can upgrade all the components in a single step, eliminating the chances of incompatibility between various components. Single bundle upgrade also ensures that your appliance runs a version that is tested and supported by Citrix. Because all the SDX components are combined in a single file, the NetScaler SDX image file is larger than the image files of NetScaler SDX release earlier than 11.0.

The file name of the image is of the format **build-sdx-11.1-<build_number>.tgz.** After the Management Service is upgraded to NetScaler SDX 11.1, the new GUI does not show the options to upload the XenServer image file, supplemental packs, or hotfixes. This happens because NetScaler SDX 11.0 does not support upgrading individual components.

- The single bundle upgrade is a multi-step process that might take up to 90 mins.
- First, the Management Service is upgraded to the newer, provided version. During the upgrade, connectivity to Management Service might be lost. Reconnect to the Management Service to monitor the status of the upgrade.
- Next, the new Management Service upgrades the XenServer and completes the remainder of the appliance upgrade. Management Service from release 11.0 and later is capable of performing full XenServer upgrade.
- Do not restart the appliance during XenServer upgrade.
- Citrix recommends that you use a XenServer serial console (or LOM console) to monitor XenServer upgrade.

If you are running version 10.5.66.x or later of the NetScaler SDX Management Service, you can use the NetScaler SDX 11.0 image file to upgrade the appliance. If your Management Service is running an older version, you must first upgrade it to version 10.5.66.x or later.

To upgrade the appliance:

1. Upload the single bundle image file, navigate to **Configuration> Management Service > Software Images** and then click **Upload**.
2. Navigate to **Configuration > System > System Administration**.
3. In the System Administration group, click **Upgrade Management Service**.

The upgrade process takes a few minutes.

Follow these steps if you upgrade from release 11.0 to a later release.

1. Upload the single bundle image file, navigate to **Configuration> Management Service > Software Images** and then click **Upload**.
2. Navigate to **Configuration > System > System Administration**.
3. In the System Administration group, click **Upgrade Appliance**.

Before the upgrade, Management Service displays the following information:

- Single bundle image file name
- The current version of NetScaler SDX running on your appliance
- The selected version to which the appliance is upgraded
- Approximate time to upgrade the appliance
- Miscellaneous information

Before clicking **Upgrade Appliance**, make sure that you have reviewed all the information displayed on the screen. You cannot abort the upgrade process once it starts.

Upgrading a NetScaler Instance

Nov 02, 2017

The process of upgrading the NetScaler instances involves uploading the build file, and then upgrading the NetScaler instance.

You have to upload the NetScaler software images to the SDX appliance before upgrading the NetScaler instances. 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.

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.

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**.

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.

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**.

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 to the SDX appliance.

Before you start upgrading any instance, ensure that you understand the licensing framework and types of licenses. 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 Management Service. 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 Management Service, downgrade the instance, and then create the LACP channels from the NetScaler VPX instance.

> **Important**
>
> Use the NetScaler Management Service only and not the VPX GUI to upgrade NetScaler VPX instances, so that during backups the upgrade images are part of the backup file. Such backup files help you restore the instance smoothly.

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 **Instance IP Address** drop-down list, select the IP addresses of the instances that you want to upgrade.
5. Click **OK**, and then click **Close**.

Managing and Monitoring the NetScaler SDX Appliance

Aug 08, 2017

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.

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.

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

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, click System > NTP Servers.

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.

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

Viewing the Properties of the NetScaler SDX Appliance

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

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

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

System Resources

Total CPU Cores

The number of CPU cores on the SDX appliance.

Total SSL Chips

The total number of SSL chips on the SDX appliance.

Free SSL chips

The total number of SSL chips that have not been assigned to a 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 NetScaler GUI click **Dashboard** and check **System Throughput (Mbps)**.

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 throughput of the SDX appliance, on the NetScaler GUI click **Dashboard** and check **System Throughput (Mbps)**.

Viewing CPU Usage for All Cores

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

The CPU Core Usage pane displays the following details:

Core Number

The CPU core number on the appliance.

Physical CPU

The physical CPU number of that core.

Hyper Threads

The hyper threads associated with that CPU core.

Instances

The instances that are using that CPU core.

Average Core Usage

The average core usage, expressed as a percentage.

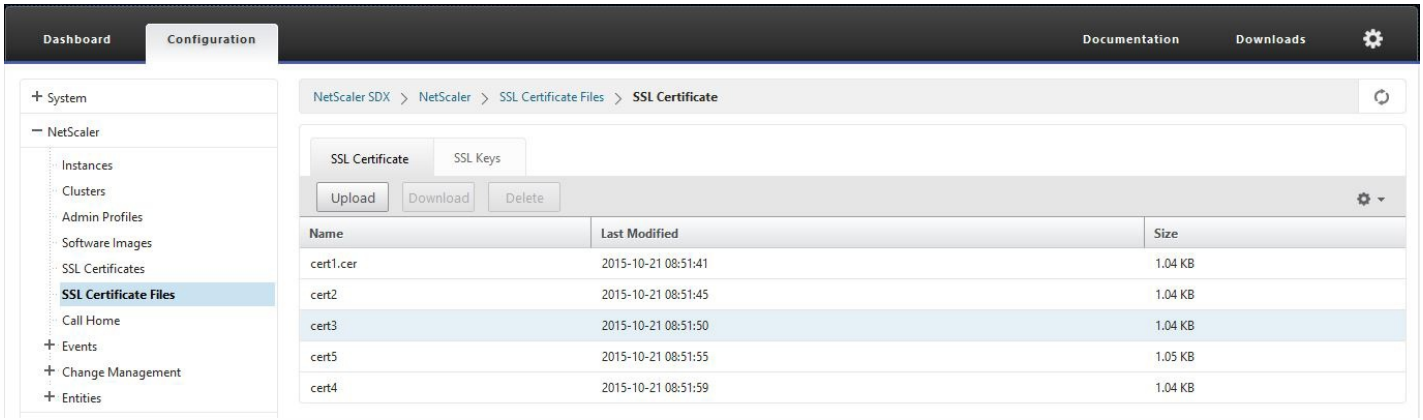
To view the CPU usage for all the cores on the SDX appliance, on the NetScaler GUI click **Dashboard** and check **System CPU Usage (%)**.

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, click System. In the Set Up Appliance group, click Install SSL Certificate and enter the details in the wizard.

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, click System and in the Set Up Appliance group, click View SSL Certificate.

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.



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.

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, click Configuration > System and in the System Administration group, click Reboot Appliance.

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

To shut down the appliance, click Configuration > System, and in the System Administration group, click Shut Down Appliance.

Creating SDX Administrative Domains

May 04, 2017

NetScaler SDX administrative domains feature helps you to create multiple administrative domains. You can use the administrative domains to segregate resources for different departments. Administrative domains can therefore improve control over resources, and the resources can be distributed among various domains for optimal use.

A NetScaler SDX appliance is shipped with fixed resources, such as CPU cores, data throughput, memory, disk space, SSL chips, and a specific number of instances that can be provisioned. The number of instances that you can create depends on the license.

A NetScaler SDX appliance supports up to three levels of administrative domains. When the appliance is shipped, all the resources are allocated to owner.

Any administrative domains that you create are subdomains of the owner domain. In each case, the subdomain's resources are allocated from the parent domain's pool of resources. The users in an administrative domain have access to that domain's resources. They do not have access to the resources of other domains at the same hierarchical level, nor to the parent-domain resources that have not been specifically allocated to their domain. However, users in a parent domain can access the resources of that domain's subdomains.

Examples of Allocating Resources to Subdomains

Table 1 lists the resources of a root domain named *nsroot* (which is the default name of the root domain). The SDX administrator can allocate these resources to subdomains. In this case, the administrator can allocate a maximum of, for example, 10 CPU cores and 840 GB of disk space.

Table 1. Owner Resources

CPU core	10
Throughput (Mbps)	18500
Memory (MB)	87300
Disk Space (GB)	840
SSL Chips	36
Instances	36

Table 2 lists the resources allocated a subdomain named *Test*. This subdomain has been allocated 5 of its parent domain's 10 CPU cores, leaving 5 cores that can be allocated to other subdomains of Owner.

Table 2. Test Domain's Resources

CPU core	5
Throughput (Mbps)	1024
Memory (MB)	2048

Disk Space (GB)	40
SSL Chips	8
Instances	4

When creating subdomains, the *Test* domain administrator can allocate only the resources listed in Table 2. The *Test* domain can have only one level of subdomains, because only three levels of domains can be created.

The following figure shows another example of resource allocation among subdomains, using different values from the ones listed in tables 1 and 2.

To create an administrative domain, navigate to Configuration > System > Administrative Domain and select the options that you want. follow the on-screen instructions. Once a new domain is created, log in to the newly created domain by using the Management Service's login page and provide the domain name and user name in the User Name field. For example, if you created a domain named NewDomain with a user NewUser then login as NewDomain\NewUser.

Assigning Users to Domains

When a sub-domain is created, two user groups are automatically created: an admin group and a read-only group. By default, each user is the part of the admin group. A user can be added to multiple groups.

Managing the RAID disk allocation

Aug 21, 2015

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 mulitple 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.

Note: RAID functionality is supported only on NetScaler SDX 22040/22060/22080/22100/22120 Platform.
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.

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 blinnk.
- 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 Addtional Logical Drive to the SDX 22000 Appliance

To add an addtional 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 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, nagivate 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.

NetScaler SDX Licensing Overview

May 04, 2017

In the NetScaler SDX Management Service, 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. For more information about the licensing portal, see "http://support.citrix.com/article/CTX131110."

To use the hardware serial number or license activation code to allocate your licenses:

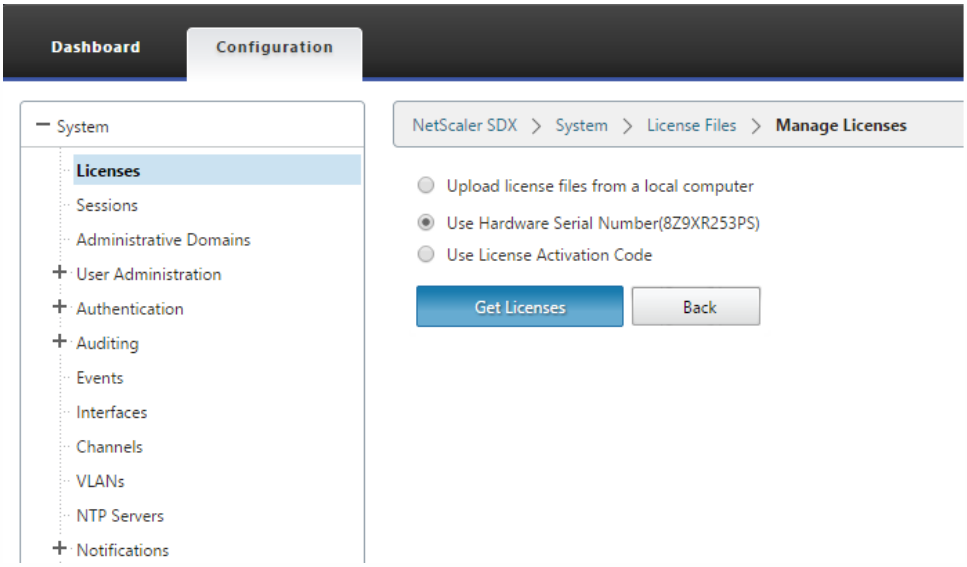
1. You must be able to access public domains through the appliance. For example, the appliance should be able to access www.citrix.com. The license allocation software internally accesses the Citrix licensing portal for your license. To access a public domain, you must configure the Management Service IP address and set up a DNS server.
2. Your license must be linked to your hardware, or you must have a valid license activation code (LAC). Citrix sends your LAC by email when you purchase a license.

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).

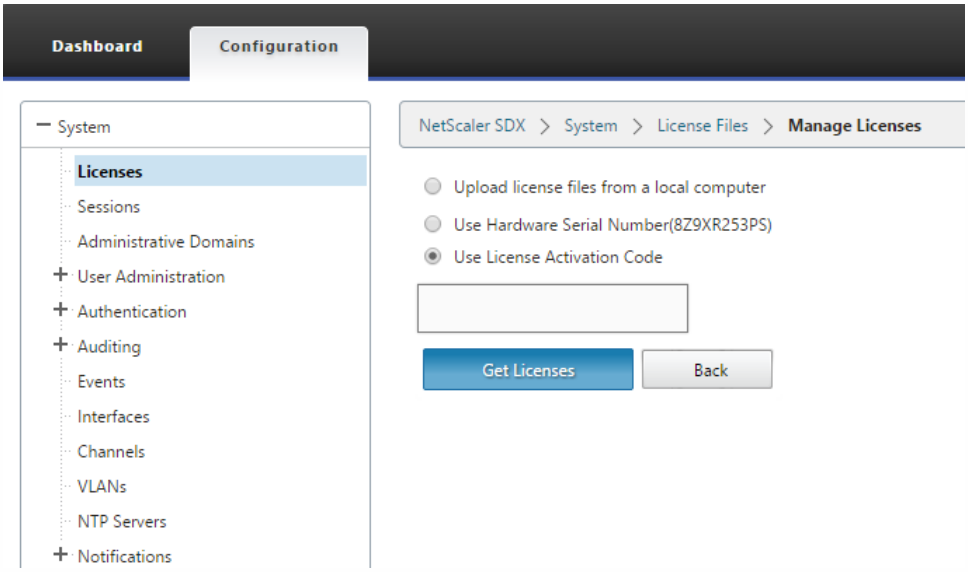
You can partially allocate licenses as required for your deployment. For example, if your license file contains ten licenses, but your current requirement is for only six licenses, you can allocate six licenses now, and allocate additional licenses later. You cannot allocate more than the total number of licenses present in your license file.

To allocate your license

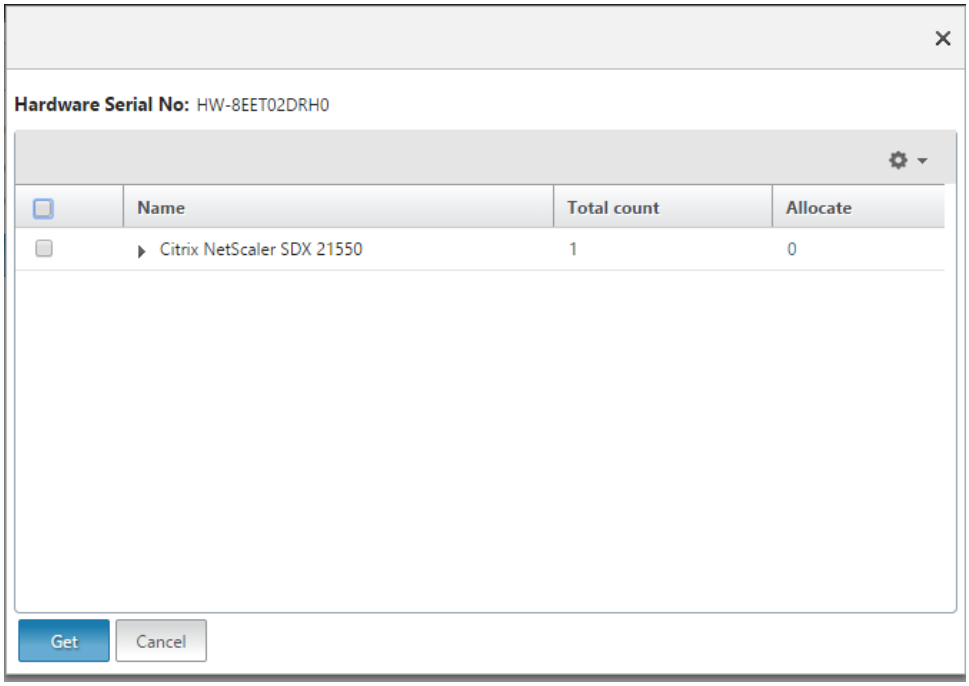
1. In a web browser, type the IP address of the Management Service of the NetScaler SDX appliance (for example, http://10.102.126.251).
2. In **User Name** and **Password**, type the administrator credentials. (default credentials—**User Name**: nsroot and **Password**: nsroot)
3. On the **Configuration** tab, navigate to **System > Licenses**.
4. In the details pane, click **Manage Licenses**, click **Add New License**, and then 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 display your license(s).



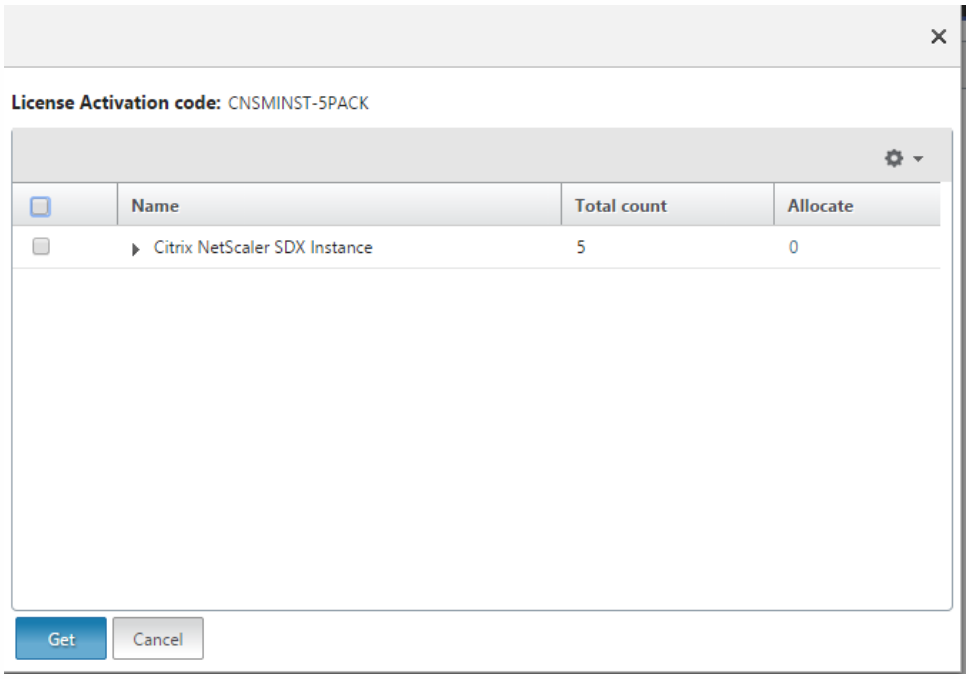
- **Use License Activation Code**—Citrix emails the LAC for the license that you purchased. Enter the LAC in the text box.



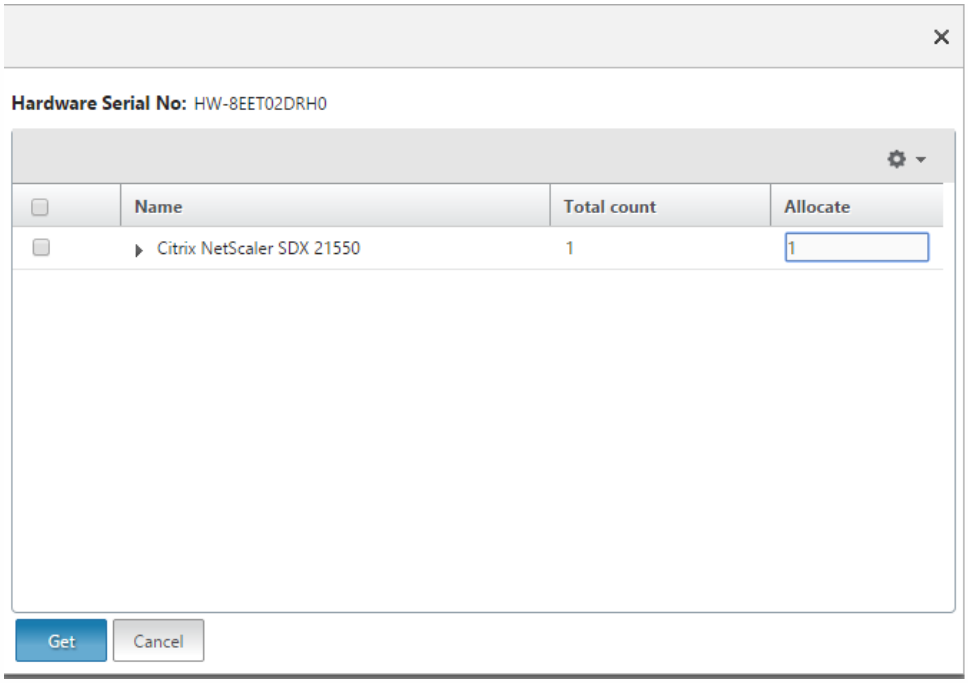
- Click **Get Licenses**. Depending on the option that you selected, one of the following dialog boxes appears.
  - The following dialog box appears if you selected **Hardware Serial Number**.



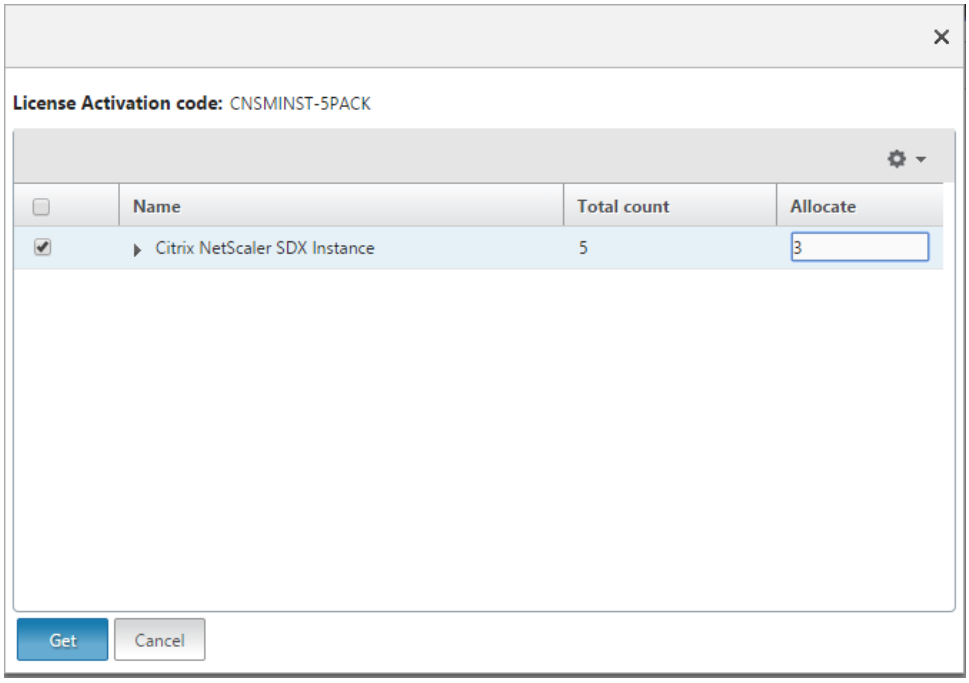
- The following dialog box appears if you selected **License Activation Code**.



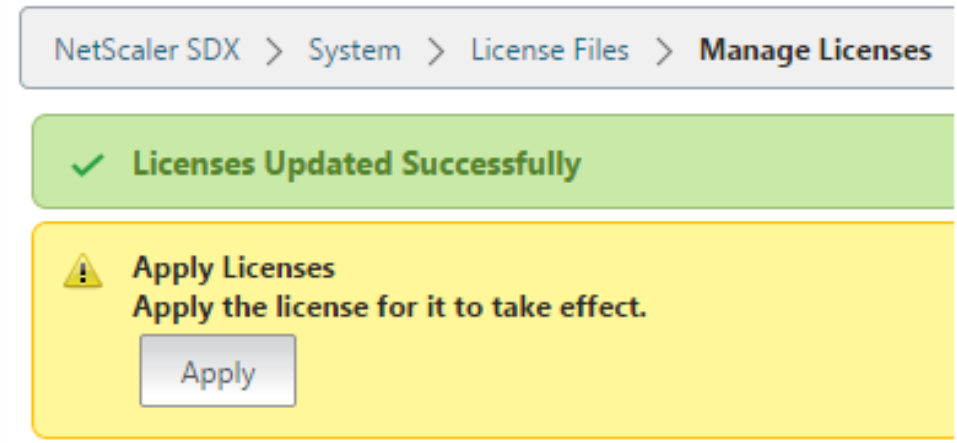
- Select the license file that you want to use to allocate your licenses.
- In the **Allocate** column, enter the number of licenses to be allocated. Then click **Get**.
  - If you selected **Hardware Serial Number**, enter the number of licenses, as shown in the following screen shot.



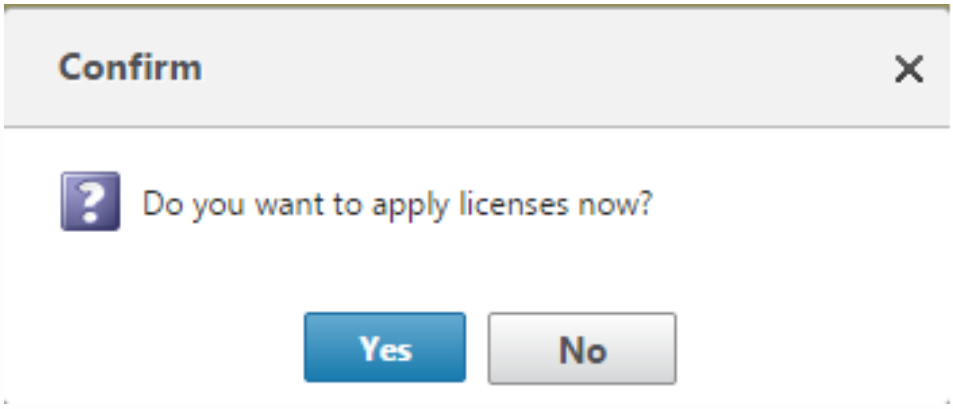
- If you selected **License Activation Code**, enter the number of licenses, as shown in the following screen shot.



- Click **Apply** for the license to take effect.



- In the **Confirm** dialog box, click **Yes** to proceed with the changes, or click **No** to cancel the changes.



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

To install a license file by using the configuration utility

1. In a web browser, type the IP address of the Management Service of the NetScaler SDX appliance (for example, http://10.102.126.251).
2. In **User Name** and **Password**, type the administrator credentials. (default credentials—**User Name**: nsroot and **Password**: nsroot)
3. On the **Configuration** tab, navigate to **System > Licenses**.
4. In the details pane, click **Manage Licenses**.
5. Click **Add New License**, then select **Upload license files from a local computer**.
6. Click **Browse**. Navigate to the location of the license files, select the license file, and then click **Open**.
7. Click **Apply** to apply the license.
8. In the **Confirm** dialog box, click **Yes** to proceed with the changes, or click **No** to cancel the changes.

SDX Resource Visualizer

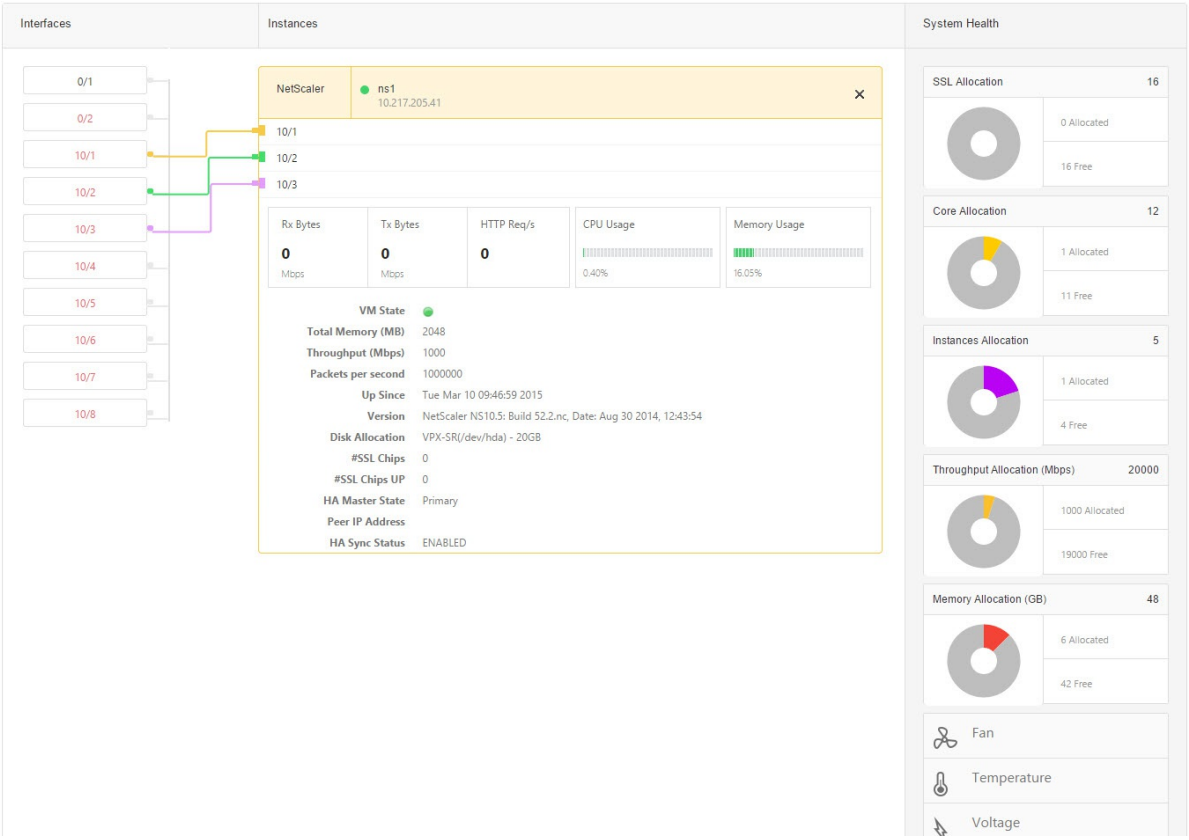
May 04, 2017

When a NetScaler instance is provisioned on NetScaler SDX, various resources such as CPU, throughput, memory need to be allocated to an instance. With current NetScaler SDX, the information about various available resources is not displayed.

Using resource visualizer, all the available resource which can be used to provision an instance are displayed in a single dashboard. All the available and used resources are shown in a graphical format. Resource visualizer also displays other parameters such as power supply status, temperature etc apart from the resources that can be allocated.

The resource visualizer also displays the various resources that an instance is using. To see the various resources associated with an instance, click on the instance name in the visualizer. The right hand side of the visualizer displays all the available and used resources in a graphical format.

The following illustration shows the details captured in resource visualizer:



Managing Interfaces

Jun 30, 2015

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.

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 Edit.
3. In the Configure Interface window, 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.

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.

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:

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

```
> show interface
1) Interface 10/3 (10G VF Interface, PF 10/4) #2
flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
MTU=1500, native vlan=1, MAC=6e:b6:f5:21:5d:db, uptime 43h03m35s
Actual: media FIBER, speed 10000, duplex FULL, fctl NONE, throughput 10000
RX: Pkts(2547925) Bytes(287996153) Errs(0) Drops(527183) Stalls(0)
TX: Pkts(196) Bytes(8532) Errs(0) Drops(0) Stalls(0)
NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
```

Bandwidth thresholds are not set.
...

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

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

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

Physical Interface	Base MAC Address
0/1	00:00:00:00:00:00
0/2	00:00:00:00:00:08
1/1	00:00:00:00:00:10
1/2	00:00:00:00:00:18
1/3	00:00:00:00:00:20
1/4	00:00:00:00:00:28
1/5	00:00:00:00:00:30
1/6	00:00:00:00:00:38
1/7	00:00:00:00:00:40
1/8	00:00:00:00:00:48
10/1	00:00:00:00:00:50
10/2	00:00:00:00:00:90

The base MAC address for the management ports is for reference only. The Management Service generates MAC addresses, on the basis of the base MAC address, for 1/x and 10/x ports only.
Note: You cannot assign a base MAC address to a channel.
To perform the various operations with MAC address, click System > Interfaces. Select an interface and then click Edit. Perform the MAC address operation, in he Configure Interface window.

Jumbo Frames on NetScaler SDX Appliances

Aug 18, 2015

NetScaler SDX appliances support receiving and transmitting jumbo frames containing up to 9216 bytes of IP data. Jumbo frames can transfer large files more efficiently than it is possible with the standard IP MTU size of 1500 bytes.

A NetScaler appliance can use jumbo frames in the following deployment scenarios:

- **Jumbo to Jumbo**: The appliance receives data as jumbo frames and sends it as jumbo frames.
- **Non-Jumbo to Jumbo**: The appliance receives data as non-jumbo frames and sends it as jumbo frames.
- **Jumbo to Non-Jumbo**: The appliance receives data as jumbo frames and sends it as non-jumbo frames.

The NetScaler instances provisioned on NetScaler SDX appliance support jumbo frames in a load balancing configuration for the following protocols:

- TCP
- Any other protocol over TCP
- SIP

For more information about jumbo frames, see the use cases.

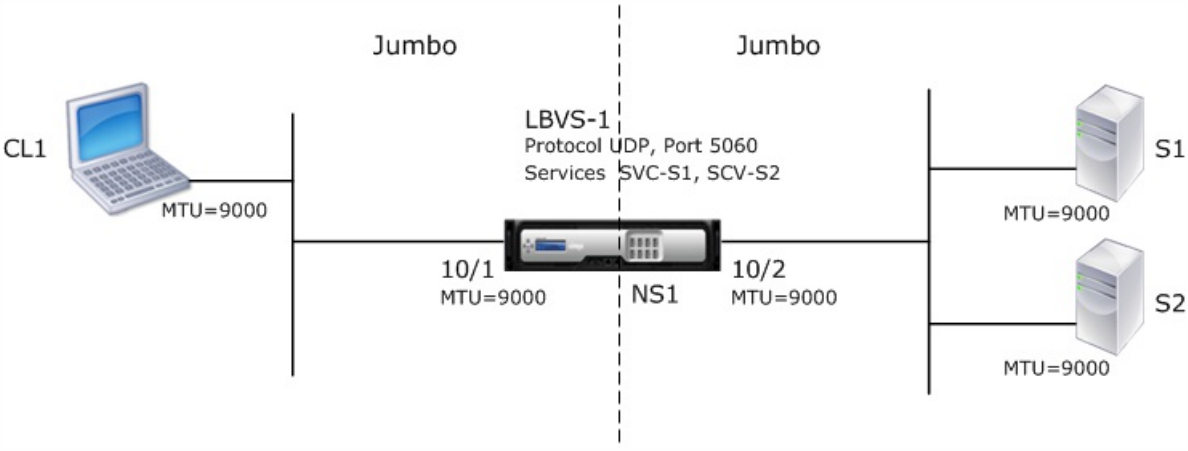
Updated: 2015-02-06

Consider an example of a jumbo to jumbo setup in which SIP load balancing virtual server LBVS-1, configured on NetScaler instance NS1, is used to load balance SIP traffic across servers S1 and S2. The connection between client CL1 and NS1, and the connection between NS1 and the servers support jumbo frames.

Interface 10/1 of NS1 receives or sends traffic from or to client CL1. Interface 10/2 of NS1 receives or sends traffic from or to server S1 or S2. Interfaces 10/1 and 10/2 of NS1 are part of VLAN 10 and VLAN 20, respectively.

For supporting jumbo frames, the MTU is set to 9216 for interfaces 10/1, 10/2, and VLANs VLAN 10, VLAN 20.

All other network devices, including CL1, S1, S2, in this setup example are also configured for supporting jumbo frames.



The following table lists the settings used in the example.

Entity	Name	Details

Entity	Name	Details
IP address of client CL1	CL1	192.0.2.10
IP address of servers	S1	198.51.100.19
	S2	198.51.100.20
MTUs specified for interfaces (by using the Management Service interface) and VLANs on NS1 (by using NetScaler command line interface).	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000
Services on NS1 representing servers	SVC-S1	• IP address: 198.51.100.19 • Protocol: SIP • Port: 5060
	SVC-S2	• IP address: 198.51.100.20 • Protocol: SIP • Port: 5060
Load balancing virtual server on VLAN 10	LBVS-1	• IP address: 203.0.113.15 • Protocol: SIP • Port: 5060 • SVC-S1, SVC-S2

Following is the traffic flow of CL1's request to NS1:

1. CL1 creates a 20000-byte SIP request for LBVS1.
2. CL1 sends the request data in IP fragments to LBVS1 of NS1. The size of each IP fragment is either equal to or less than the MTU (9000) set on the interface from which CL1 sends these fragments to NS1.
   - Size of the first IP fragment = [IP header + UDP header + SIP data segment] = [20 + 8 + 8972] = 9000
   - Size of the second IP fragment = [IP header + SIP data segment] = [20 + 8980] = 9000
   - Size of the last IP fragment=[IP header + SIP data segment] = [20 + 2048] = 2068
3. NS1 receives the request IP fragments at interface 10/1. NS1 accepts these fragments, because the size of each of these fragments is equal to or less than the MTU (9000) of interface 10/1.
4. NS1 reassembles these IP fragments to form the 27000-byte SIP request. NS1 processes this request.
5. LBVS-1's load balancing algorithm selects server S1.
6. NS1 sends the request data in IP fragments to S1. The size of each IP fragment is either equal or less than the MTU (9000) of the interface 10/2, from which NS1 sends these fragments to S1. The IP packets are sourced with a SNIP

address of NS1.

- Size of the first IP fragment = [IP header + UDP header + SIP data segment] = [20 + 8 + 8972] = 9000
- Size of the second IP fragment = [IP header + SIP data segment] = [20 + 8980] = 9000
- Size of the last IP fragment=[IP header + SIP data segment] = [20 + 2048] = 2068

Following is the traffic flow of S1's response to CL1 in this example:

1. Server S1 creates a 30000-byte SIP response to send to the SNIP address of NS1.
2. S1 sends the response data in IP fragments to NS1. The size of each IP fragment is either equal to or less than the MTU (9000) set on the interface from which S1 sends these fragments to NS1.
   - Size of the first IP fragment = [IP header + UDP header + SIP data segment] = [20 + 8 + 8972] = 9000
   - Size of the second and third IP fragment = [IP header + SIP data segment] = [20 + 8980] = 9000
   - Size of the last IP fragment=[IP header + SIP data segment] = [20 + 3068] = 3088
3. NS1 receives the response IP fragments at interface 10/2. NS1 accepts these fragments, because the size of each fragment is equal to or less than the MTU (9000) of interface 10/2.
4. NS1 reassembles these IP fragments to form the 27000-byte SIP response. NS1 processes this response.
5. NS1 sends the response data in IP fragments to CL1. The size of each IP fragment is either equal or less than the MTU (9000) of the interface 10/1, from which NS1 sends these fragments to CL1. The IP fragments are sourced with LBVS-1's IP address. These IP packets are sourced from LBVS-1's IP address and destined to CL1's IP address.
   - Size of the first IP fragment = [IP header + UDP header + SIP data segment] = [20 + 8 + 8972] = 9000
   - Size of the second and third IP fragment = [IP header + SIP data segment] = [20 + 8980] = 9000

Size of the last IP fragment=[IP header + SIP data segment] = [20 + 3068] = 3088

Configuration Tasks

On the NetScaler SDX Management Service, navigate to Configuration > System > Interfaces page. Select the required interface and click Edit. Set the MTU value and click OK.

Example

Set the MTU value for interface 10/1 as 9000 and for interface 10/2 as 9000.

Log on to NetScaler instance and use the NetScaler command line interface to complete the remaining configuration steps.

The following table list the tasks, NetScaler commands, and examples for creating the required configuration on the NetScaler instances.

Tasks	NetScaler Command Syntax	Examples
Create VLANs and set the MTU of the desired VLANs for supporting jumbo frames.	add vlan <id> -mtu <positive_integer> show vlan <id>	add vlan 10 -mtu 9000 add vlan 20 -mtu 9000
Bind interfaces to VLANs.	bind vlan <id> -ifnum <interface_name>	bind vlan 10 -ifnum 10/1 bind vlan 20 -ifnum 10/2

Tasks	NetScaler Command Syntax	Examples
	show vlan <id>	
Add a SNIP address.	add ns ip <IPAddress> <netmask> -type SNIP show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Create services representing SIP servers.	add service <serviceName> <ip> SIP_UDP <port> show service <name>	add service SVC-S1 198.51.100.19 SIP_UDP 5060 dd service SVC-S2 198.51.100.20 SIP_UDP 5060
Create SIP load balancing virtual servers and bind the services to it	add lb vserver <name> SIP_UDP <ip> <port> bind lb vserver <vserverName> <serviceName> show lb vserver <name>	add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060 bind lb vserver LBVS-1 SVC-S1 bind lb vserver LBVS-1 SVC-S2
bind lb vserver LBVS-1 SVC-S2	save ns config show ns config	

Updated: 2015-02-06

Consider an example of a non-jumbo to jumbo setup in which load balancing virtual server LBVS1, configured on a NetScaler instance NS1, is used to load balance traffic across servers S1 and S2. The connection between client CL1 and NS1 supports non-jumbo frames, and the connection between NS1 and the servers supports jumbo frames.

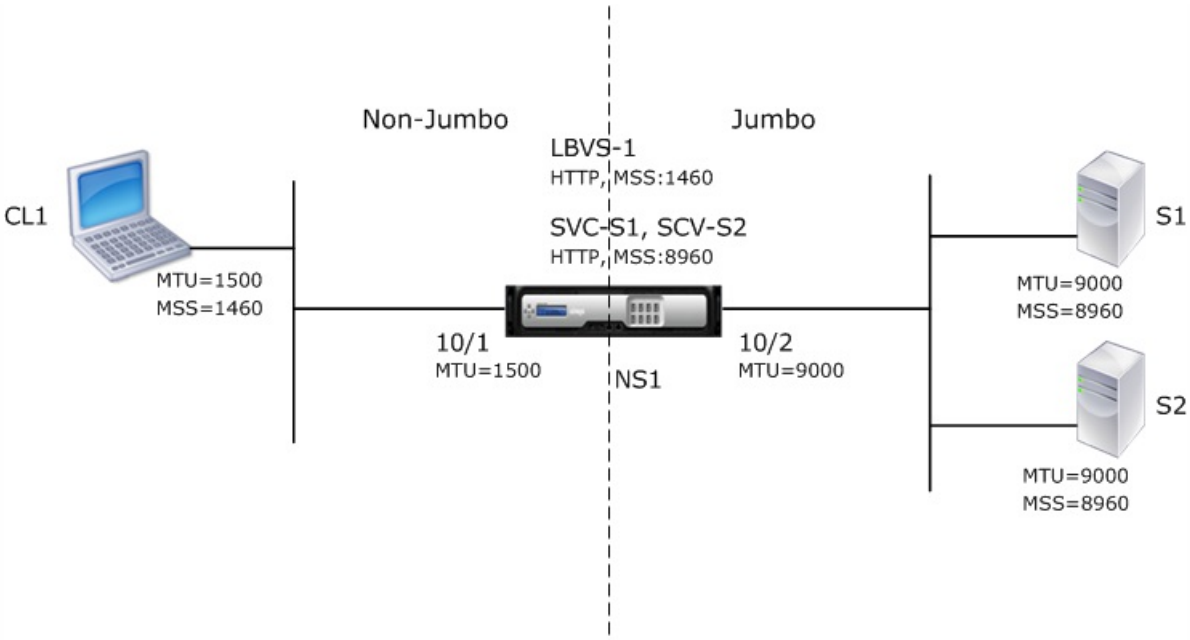
Interface 10/1 of NS1 receives or sends traffic from or to client CL1. Interface 10/2 of NS1 receives or sends traffic from or to server S1 or S2.

Interfaces 10/1 and 10/2 of NS1 are part of VLAN 10 and VLAN 20, respectively. For supporting only non-jumbo frames between CL1 and NS1, the MTU is set to the default value of 1500 for both interface 10/1 and VLAN 10.

For supporting jumbo frames between NS1 and the servers, the MTU is set to 9000 for interface 10/2 and VLAN 20.

Servers and all other network devices between NS1 and the servers are also configured for supporting jumbo frames. Since HTTP traffic is based on TCP, MSSs are set accordingly at each end point for supporting jumbo frames:

- For the connection between CL1 and virtual server LBVS1 of NS1, the MSS on NS1 is set in a TCP profile, which is then bound to LBVS1.
- For the connection between a SNIP address of NS1 and S1, the MSS on NS1 is set in a TCP profile, which is then bound to the service (SVC-S1) representing S1 on NS1.



The following table lists the settings used in this example:

Entity	Name	Details
IP address of client CL1	CL1	192.0.2.10
IP address of servers	S1	198.51.100.19
	S2	198.51.100.20
MTU for interface 10/1 (by using the Management Service interface).		1500
MTU set for interface 10/2(by using the Management Service interface).		9000
MTU for VLAN 10 on NS1 (by using NetScaler command line interface).		1500
MTU set for VLAN 20 on NS1 (by using NetScaler command line interface).		9000
Services on NS1 representing servers	SVC-S1	• IP address: 198.51.100.19 • Protocol: HTTP • Port: 80 • MSS: 8960
	SVC-S2	• IP address: 198.51.100.20 • Protocol: HTTP • Port: 80 • MSS: 8960
Load balancing virtual server on VLAN 10	LBVS-1	• IP address: 203.0.113.15 • Protocol: HTTP

Entity	Name	Details
		• Port: 80 • Bound services: SVC-S1, SVC-S2 • MSS: 1460

Following is the traffic flow of CL1's request to S1 in this example:

1. Client CL1 creates a 200-byte HTTP request to send to virtual server LBVS-1 of NS1.
2. CL1 opens a connection to LBVS-1 of NS1. CL1 and NS1 exchange their respective TCP MSS values while establishing the connection.
3. Because NS1's MSS is larger than the HTTP request, CL1 sends the request data in a single IP packet to NS1.
    1. Size of the request packet = [IP Header + TCP Header + TCP Request] = [20 + 20 + 200] = 240
4. NS1 receives the request packet at interface 10/1 and then processes the HTTP request data in the packet.
5. LBVS-1's load balancing algorithm selects server S1, and NS1 opens a connection between one of its SNIP addresses and S1. NS1 and CL1 exchange their respective TCP MSS values while establishing the connection.
6. Because S1's MSS is larger than the HTTP request, NS1 sends the request data in a single IP packet to S1.
    1. Size of the request packet = [IP Header + TCP Header + [TCP Request] = [20 + 20 + 200] = 240

Following is the traffic flow of S1's response to CL1 in this example:

1. Server S1 creates an 18000-byte HTTP response to send to the SNIP address of NS1.
2. S1 segments the response data into multiples of NS1's MSS and sends these segments in IP packets to NS1. These IP packets are sourced from S1's IP address and destined to the SNIP address of NS1.
    - Size of the first two packet = [IP Header + TCP Header + (TCP segment=NS1's MSS size)] = [20 + 20 + 8960] = 9000
    - Size of the last packet = [IP Header + TCP Header + (remaining TCP segment)] = [20 + 20 + 2080] = 2120
3. NS1 receives the response packets at interface 10/2.
4. From these IP packets, NS1 assembles all the TCP segments to form the HTTP response data of 18000 bytes. NS1 processes this response.
5. NS1 segments the response data into multiples of CL1's MSS and sends these segments in IP packets, from interface 10/1, to CL1. These IP packets are sourced from LBVS-1's IP address and destined to CL1's IP address.
    - Size of all the packet except the last = [IP Header + TCP Header + (TCP payload=CL1's MSS size)] = [20 + 20 + 1460] = 1500
    - Size of the last packet = [IP Header + TCP Header + (remaining TCP segment)] = [20 + 20 + 480] = 520

Configuration Tasks

On the NetScaler SDX Management Service, navigate to Configuration > System > Interfaces page. Select the required interface and click Edit. Set the MTU value and click OK.

Example

Set the following MTU values:

- For 10/1 interface as 1500
- For 10/2 interface as 9000

Log on to NetScaler instance and use the NetScaler command line interface to complete the remaining configuration steps.

The following table list the tasks, NetScaler commands, and examples for creating the required configuration on the NetScaler instances.

Tasks	NetScaler Command Line Syntax	Example
Create VLANs and set the MTU of the desired VLANs for supporting jumbo frames.	add vlan <id> -mtu <positive_integer> show vlan <id>	add vlan 10 -mtu 1500 add vlan 20 -mtu 9000
Bind interfaces to VLANs.	bind vlan <id> -ifnum <interface_name> show vlan <id>	bind vlan 10 -ifnum 10/1 bind vlan 20 -ifnum 10/2
Add a SNIP address.	add ns ip <IPAddress> <netmask> -type SNIP show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Create services representing HTTP servers	add service <serviceName> <ip> HTTP <port> show service <name>	add service SVC-S1 198.51.100.19 http 80 add service SVC-S2 198.51.100.20 http 80
Create HTTP load balancing virtual servers and bind the services to it	add lb vserver <name> HTTP <ip> <port> bind lb vserver <vserverName> <serviceName> show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80 bind lb vserver LBVS-1 SVC-S1
Create a custom TCP profile and set its MSS for supporting jumbo frames.	add tcpProfile <name> -mss <positive_integer> show tcpProfile <name>	add tcpprofile NS1-SERVERS-JUMBO -mss 8960
Bind the custom TCP profile to the desired services.	set service <Name> -tcpProfileName <string> show service <name>	set service SVC-S1 -tcpProfileName NS1- SERVERS-JUMBO set service SVC-S2 -tcpProfileName NS1- SERVERS-JUMBO
Save the configuration	save ns config	

Tasks	NetScaler Command Line Syntax	Example
	show ns config	

Updated: 2015-04-14

Consider an example in which load balancing virtual servers LBVS1 and LBVS2 are configured on NetScaler instance NS1. LBVS1 is used to load balance HTTP traffic across servers S1 and S2, and global is used to load balance traffic across servers S3 and S4.

CL1 is on VLAN 10, S1 and S2 are on VLAN20, CL2 is on VLAN 30, and S3 and S4 are on VLAN 40. VLAN 10 and VLAN 20 support jumbo frames, and VLAN 30 and VLAN 40 support only non-jumbo frames.

In other words, the connection between CL1 and NS1, and the connection between NS1 and server S1 or S2 support jumbo frames. The connection between CL2 and NS1, and the connection between NS1 and server S3 or S4 support only non-jumbo frames.

Interface 10/1 of NS1 receives or sends traffic from or to clients. Interface 10/2 of NS1 receives or sends traffic from or to the servers.

Interface 10/1 is bound to both VLAN 10 and VLAN 20 as a tagged interface, and interface 10/2 is bound to both VLAN 30 and VLAN 40 as a tagged interface.

For supporting jumbo frames, the MTU is set to 9216 for interfaces 10/1 and 10/2.

On NS1, the MTU is set to 9000 for VLAN 10 and VLAN 30 for supporting jumbo frames, and the MTU is set to the default value of 1500 for VLAN 20 and VLAN 40 for supporting only non-jumbo frames.

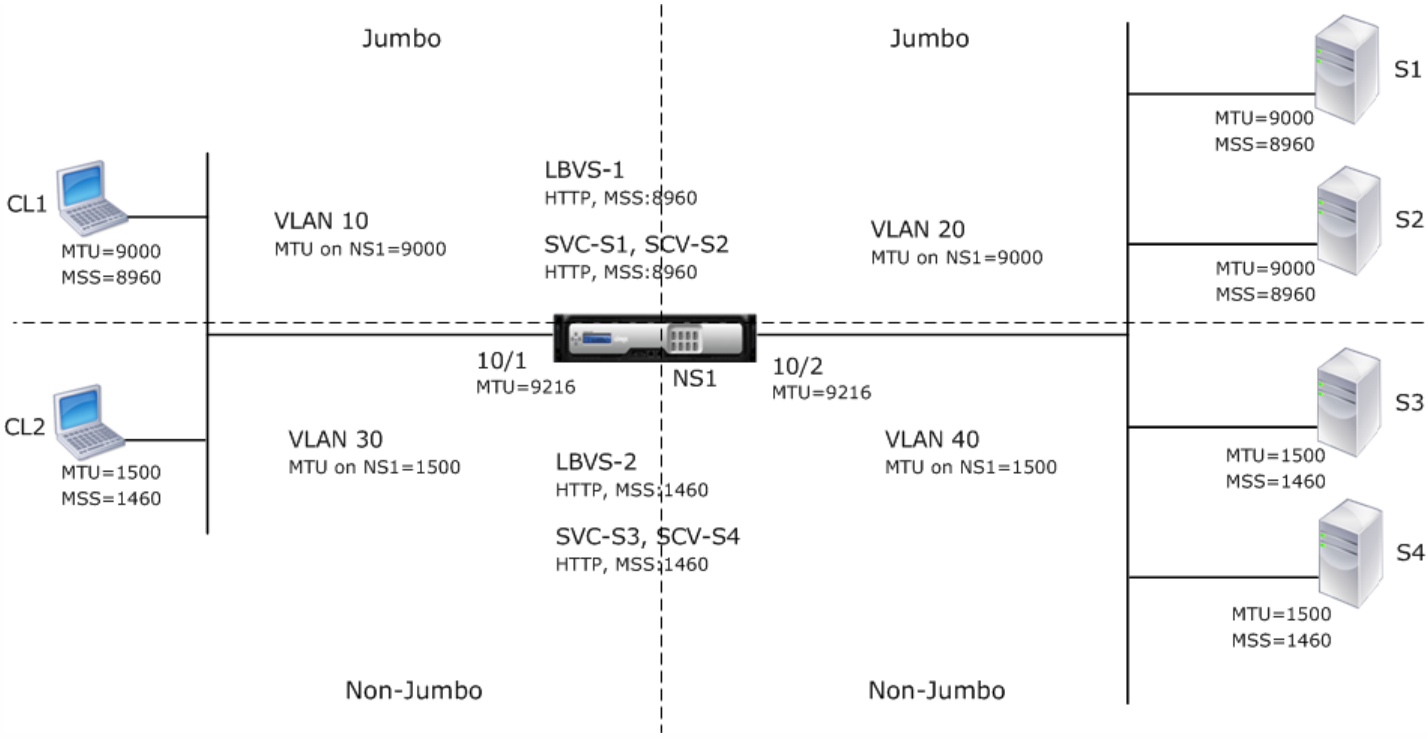
The effective MTU on a NetScaler interface for VLAN tagged packets is of the MTU of the interface or the MTU of the VLAN, whichever is lower. For example:

- The MTU of interface 10/1 is 9216. The MTU of VLAN 10 is 9000. On interface 10/1, the MTU of VLAN 10 tagged packets is 9000.
- The MTU of interface 10/2 is 9216. The MTU of VLAN 20 is 9000. On interface 10/2, the MTU of VLAN 20 tagged packets is 9000.
- The MTU of interface 10/1 is 9216. The MTU of VLAN 30 is 1500. On interface 10/1, the MTU of VLAN 30 tagged packets is 1500.
- The MTU of interface 10/2 is 9216. The MTU of VLAN 40 is 1500. On interface 10/2, the MTU of VLAN 40 tagged packets is 9000.

CL1, S1, S2, and all network devices between CL1 and S1 or S2 are configured for jumbo frames.

Since HTTP traffic is based on TCP, MSSs are set accordingly at each end point for supporting jumbo frames.

- For the connection between CL1 and virtual server LBVS-1 of NS1, the MSS on NS1 is set in a TCP profile, which is then bound to LBVS1.
- For the connection between a SNIP address of NS1 and S1, the MSS on NS1 is set in a TCP profile, which is then bound to the service (SVC-S1) representing S1 on NS1.



The following table lists the settings used in this example.

Entity	Name	Details
IP address of clients	CL1	192.0.2.10
	CL2	192.0.2.20
IP address of servers	S1	198.51.100.19
	S2	198.51.100.20
	S3	198.51.101.19
	S4	198.51.101.20
SNIP addresses on NS1		• 198.51.100.18 • 198.51.101.18
MTU specified for interfaces and VLANs on NS1	10/1	9216
	10/2	9216
	VLAN 10	9000
	VLAN 20	9000
	VLAN 30	9000
	VLAN 40	1500

Entity	Name	Details
Default TCP profile	nstcp_default_profile	MSS: 1460
Custom TCP profile	ALL-JUMBO	MSS: 8960
Services on NS1 representing servers	SVC-S1	• IP address: 198.51.100.19 • Protocol: HTTP • Port: 80 • TCP profile: ALL-JUMBO (MSS: 8960)
	SVC-S2	• IP address: 198.51.100.20 • Protocol: HTTP • Port: 80 • TCP profile: ALL-JUMBO (MSS: 8960)
	SVC-S3	• IP address: 198.51.101.19 • Protocol: HTTP • Port: 80 • TCP profile: nstcp_default_profile (MSS:1460)
	SVC-S4	• IP address: 198.51.101.20 • Protocol: HTTP • Port: 80 • TCP profile: nstcp_default_profile (MSS:1460)
Load balancing virtual servers on NS1	LBVS-1	• IP address = 203.0.113.15 • Protocol: HTTP • Port:80 • Bound services: SVC-S1, SVC-S2 • TCP profile: ALL-JUMBO (MSS: 8960)
	LBVS-2	• IP address = 203.0.114.15 • Protocol: HTTP • Port:80 • Bound services: SVC-S3, SVC-S4 • TCP Profile: nstcp_default_profile (MSS:1460)

Following is the traffic flow of CL1's request to S1:

1. Client CL1 creates a 20000-byte HTTP request to send to virtual server LBVS-1 of NS1.
2. CL1 opens a connection to LBVS-1 of NS1. CL1 and NS1 exchange their TCP MSS values while establishing the connection.
3. Because NS1's MSS value is smaller than the HTTP request, CL1 segments the request data into multiples of NS1's MSS

and sends these segments in IP packets tagged as VLAN 10 to NS1.
   - Size of the first two packets = [IP Header + TCP Header + (TCP segment=NS1 MSS)] = [20 + 20 + 8960] = 9000
   - Size of the last packet = [IP Header + TCP Header + (remaining TCP segment)] = [20 + 20 + 2080] = 2120
4. NS1 receives these packets at interface 10/1. NS1 accepts these packets because the size of these packets is equal to or less than the effective MTU (9000) of interface 10/1 for VLAN 10 tagged packets.
5. From the IP packets, NS1 assembles all the TCP segments to form the 20000-byte HTTP request. NS1 processes this request.
6. LBVS-1's load balancing algorithm selects server S1, and NS1 opens a connection between one of its SNIP addresses and S1. NS1 and CL1 exchange their respective TCP MSS values while establishing the connection.
7. NS1 segments the request data into multiples of S1's MSS and sends these segments in IP packets tagged as VLAN 20 to S1.
   - Size of the first two packets = [IP Header + TCP Header + (TCP payload=S1 MSS)] = [20 + 20 + 8960] = 9000
   - Size of the last packet = [IP Header + TCP Header + (remaining TCP segment)] = [20 + 20 + 2080] = 2120

Following is the traffic flow of S1's response to CL1:

1. Server S1 creates a 30000-byte HTTP response to send to the SNIP address of NS1.
2. S1 segments the response data into multiples of NS1's MSS and sends these segments in IP packets tagged as VLAN 20 to NS1. These IP packets are sourced from S1's IP address and destined to the SNIP address of NS1.
   - Size of first three packet = [IP Header + TCP Header + (TCP segment=NS1's MSS size)] = [20 + 20 + 8960] = 9000
   - Size of the last packet = [IP Header + TCP Header + (remaining TCP segment)] = [20 + 20 + 3120] = 3160
3. NS1 receives the response packets at interface 10/2. NS1 accepts these packets, because their size is equal to or less than the effective MTU value (9000) of interface 10/2 for VLAN 20 tagged packets.
4. From these IP packets, NS1 assembles all the TCP segments to form the 30000-byte HTTP response. NS1 processes this response.
5. NS1 segments the response data into multiples of CL1's MSS and sends these segments in IP packets tagged as VLAN 10, from interface 10/1, to CL1. These IP packets are sourced from LBVS's IP address and destined to CL1's IP address.
   - Size of first three packet = [IP Header + TCP Header + [(TCP payload=CL1's MSS size)] = [20 + 20 + 8960] = 9000
   - Size of the last packet = [IP Header + TCP Header + (remaining TCP segment)] = [20 + 20 + 3120] = 3160

Configuration Tasks

On the NetScaler SDX Management Service, navigate to Configuration > System > Interfaces page. Select the required interface and click Edit. Set the MTU value and click OK.

Example:

Set the following MTU values:

- For 10/1 interface as 9216
- For 10/2 interface as 9216

Log on to NetScaler instance and use the NetScaler command line interface to complete the remaining configuration steps.

The following table list the tasks, NetScaler commands, and examples for creating the required configuration on the NetScaler instances.

Task	Syntax	Example
Create VLANs and set the MTU of the desired	add vlan <id> -mtu	add vlan 10 -mtu 9000

Task	Syntax	Example
VLANs for supporting jumbo frames.	<positive_integer> show vlan <id>	add vlan 20 -mtu 9000 add vlan 30 -mtu 1500 add vlan 40 -mtu 1500
Bind interfaces to VLANs.	bind vlan <id> -ifnum <interface_name> show vlan <id>	bind vlan 10 -ifnum 10/1 -tagged bind vlan 20 -ifnum 10/2 -tagged bind vlan 30 -ifnum 10/1 -tagged bind vlan 40 -ifnum 10/2 -tagged
Add a SNIP address.	add ns ip <IPAddress> <netmask> -type SNIP show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP add ns ip 198.51.101.18 255.255.255.0 -type SNIP
Create services representing HTTP servers.	add service <serviceName> <ip> HTTP <port> show service <name>	add service SVC-S1 198.51.100.19 http 80 add service SVC-S2 198.51.100.20 http 80 add service SVC-S3 198.51.101.19 http 80 add service SVC-S4 198.51.101.20 http 80
Create HTTP load balancing virtual servers and bind the services to it	add lb vserver <name> HTTP <ip> <port> bind lb vserver <vserverName> <serviceName> show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80 bind lb vserver LBVS-1 SVC-S1 bind lb vserver LBVS-1 SVC-S2
		add lb vserver LBVS-2 http

Task	Syntax	Example
		203.0.114.15 80 bind lb vserver LBVS-2 SVC-S3 bind lb vserver LBVS-2 SVC-S4
Create a custom TCP profile and set its MSS for supporting jumbo frames.	add tcpProfile <name> -mss <positive_integer> show tcpProfile <name>	add tcpprofile ALL-JUMBO -mss 8960
Bind the custom TCP profile to the desired load balancing virtual server and services.	set service <Name> -tcpProfileName <string> show service <name>	set lb vserver LBVS-1 -tcpProfileName ALL-JUMBO set service SVC-S1 -tcpProfileName ALL-JUMBO set service SVC-S2 -tcpProfileName ALL-JUMBO
Save the configuration	save ns config show ns config	

Configuring SNMP on NetScaler SDX Appliances

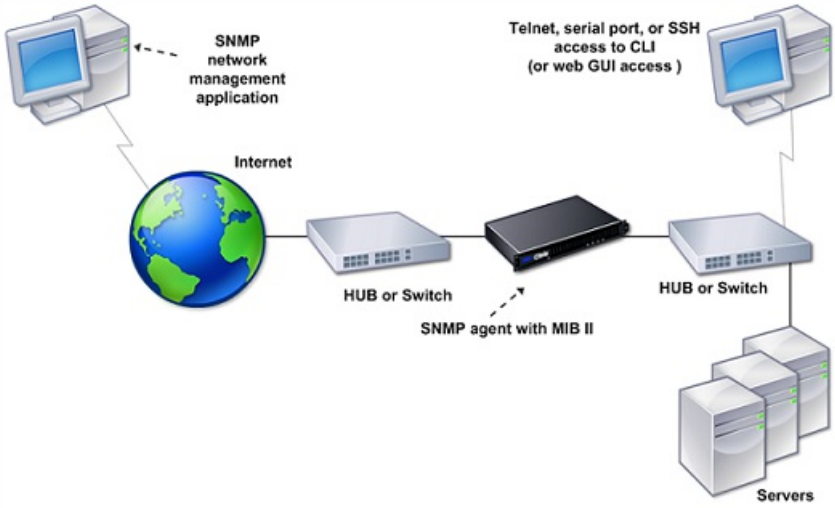
May 04, 2017

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.

In addition to configuring an SNMP trap destination, downloading MIB files, and configuring one or more SNMP managers, you can configure the NetScaler appliance for SNMPv3 queries.

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.

1. On the configuration tab, in the navigation pane, expand System > SNMP, and then click SNMP Trap Destinations.
2. In the SNMP Trap Destinations pane, click Add.
3. In the Configure SNMP Trap Destination page, 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.

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.

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 Create SNMP Manager Communitypage, 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.

Simple Network Management Protocol Version 3 (SNMPv3) is based on the basic structure and architecture of SNMPv1 and SNMPv2. However, SNMPv3 enhances the basic architecture to incorporate administration and security capabilities, such as authentication, access control, data integrity check, data origin verification, message timeliness check, and data confidentiality.

The Citrix NetScaler SDX appliance supports the following entities that enable you to implement the security features of SNMPv3:

- SNMP Views
- SNMP Users

These entities function together to implement the SNMPv3 security features. Views are created to allow access to subtrees of the MIB.

Adding an SNMP Manager

You must configure the CloudBridge 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. Navigate to the System > Configuration page.
2. On the Configuration tab, in the navigation pane, expand System, and then expand SNMP.
3. Click Managers.
4. In the details pane, click Add.
5. 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.
6. Click Add, and then click Close.

SNMP views restrict user access to specific portions of the MIB. SNMP views are used to implement access control.

To configure a view

1. On the Configuration tab, in the navigation pane, expand System, and then expand SNMP.
2. Click Views.
3. In the details pane, click Add.
4. In the Add SNMP View dialog box, set the following parameters:
   - Name—Name for the SNMPv3 view. 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. You should choose a name that helps identify the SNMPv3 view.
   - Subtree—A particular branch (subtree) of the MIB tree, which you want to associate with this SNMPv3 view. You must specify the subtree as an SNMP OID.
   - Type—Include or exclude the subtree, specified by the subtree parameter, in or from this view. This setting can be useful when you have included a subtree, such as A, in an SNMPv3 view and you want to exclude a specific subtree of A, such as B, from the SNMPv3 view.

After you have created an SNMP view, add SNMP users. SNMP users have access to the MIBs that are required for querying the SNMP managers.

To configure a user

1. On the Configuration tab, in the navigation pane, expand System, and then expand SNMP.
2. Click Users.
3. In the details pane, click Add.
4. In the Create SNMP Userpage, set the following parameters:
   - Name—Name for the SNMPv3 user. 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.
   - Security Level—Security level required for communication between the appliance and the SNMPv3 users. Select from one of the following options:
     - noAuthNoPriv—Require neither authentication nor encryption.
     - authNoPriv—Require authentication but no encryption.
     - authPriv—Require authentication and encryption.
   - Authentication Protocol—Authentication algorithm used by the appliance and the SNMPv3 user for authenticating the communication between them. You must specify the same authentication algorithm when you configure the SNMPv3 user in the SNMP manager.
   - Authentication Password—Pass phrase to be used by the authentication algorithm. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters.
   - Privacy Protocol—Encryption algorithm used by the appliance and the SNMPv3 user for encrypting the communication between them. You must specify the same encryption algorithm when you configure the SNMPv3 user in the SNMP manager.
   - View Name—Name of the configured SNMPv3 view that you want to bind to this SNMPv3 user. An SNMPv3 user can access the subtrees that are bound to this SNMPv3 view as type INCLUDED, but cannot access the ones that are type EXCLUDED.

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, click System > SNMP > Alarms.

Configuring Syslog Notifications

May 04, 2017

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.

1. Navigate to System > Notifications > Syslog Servers.
2. In the details pane, click Add.
3. In the Create Syslog Serverpage, 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.

1. Navigate to System > Notifications > Syslog Servers.
2. In the details pane, click Syslog Parameters.
3. In the Configure Syslog Parameterspage, specify the date and time format.
4. Click OK, and then click Close.

Configuring Mail Notifications

May 04, 2017

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 > Email.
2. In the details pane, click Email Server, and then click Add.
3. In the Create Email Server page, 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 > Email.
2. In the details pane, click Email Distribution List, and then click Add.
3. In the Create Email Distribution Listpage, 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

May 04, 2017

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 Create SMS Serverpage, specify values for the SMS server parameters. The values for these parameters are provided by the vendor.
4. Click Create, and then click Close.

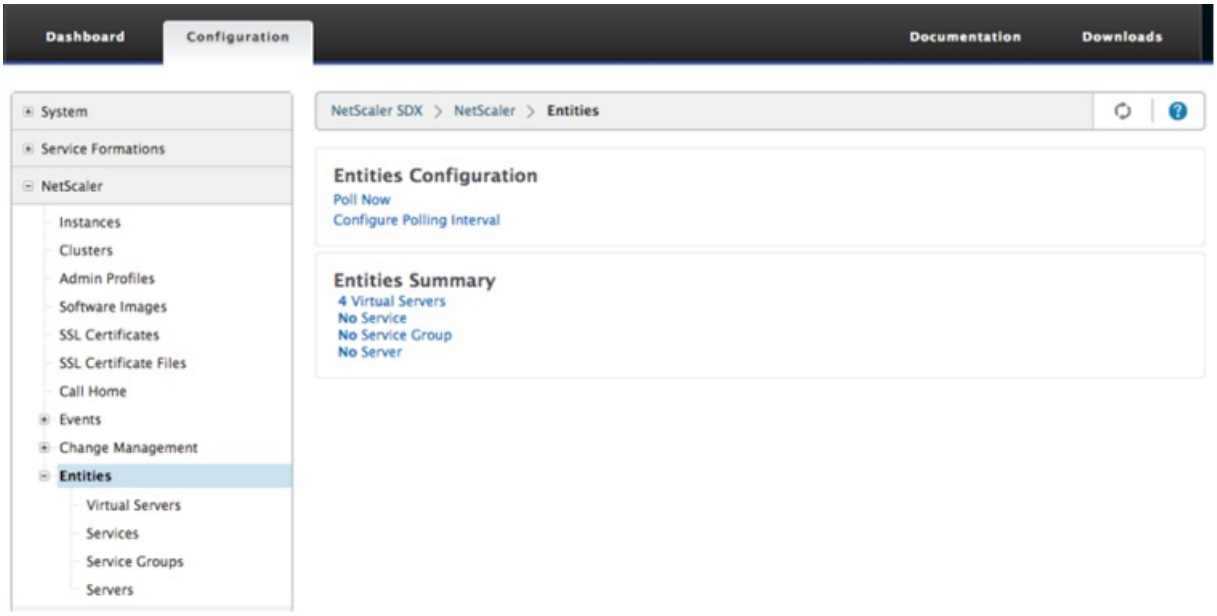
To configure an SMS profile

1. Navigate to System > Notifications > SMS.
2. In the details pane, click SMS Distribution List, and then click Add.
3. In the Create SMS Distribution List page, 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

May 04, 2017

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.



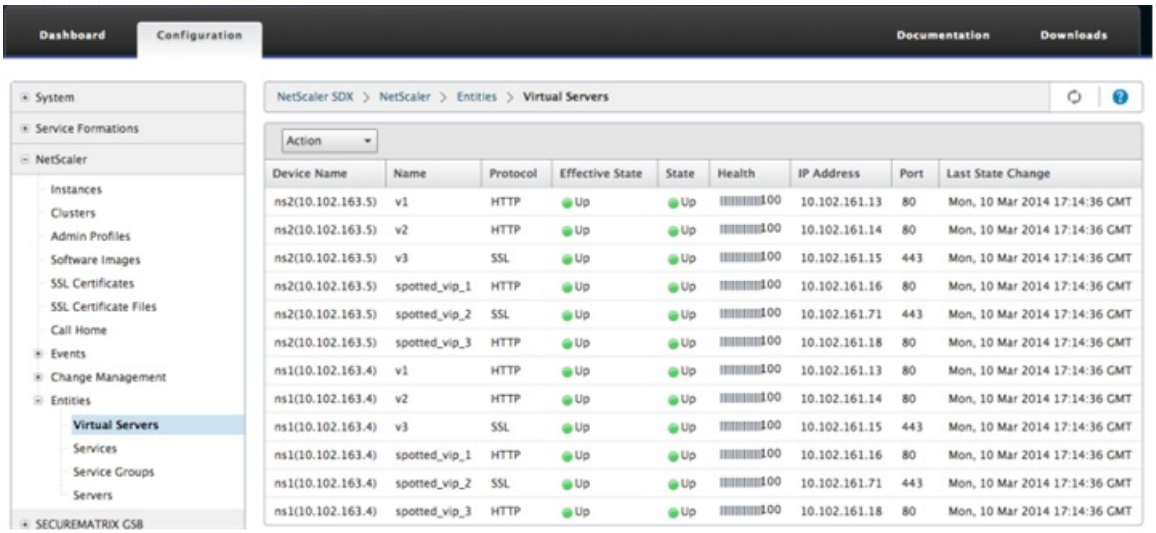
Viewing the Status of Virtual Servers

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: (Number of bound UP services * 100) / Total bound services
   - IP Address—IP address of the virtual server. Clients send connection requests to this IP address.
   - Port—ort on which the virtual server listens for client conections.
   - 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.

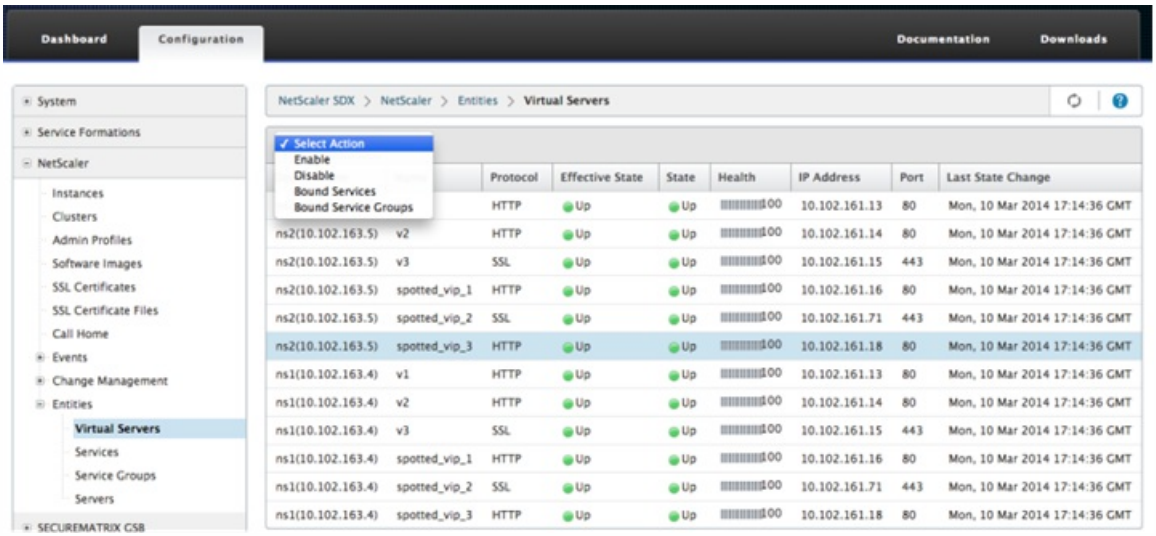


Viewing Services and Service Groups Bound to a Virtual Server

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.



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:

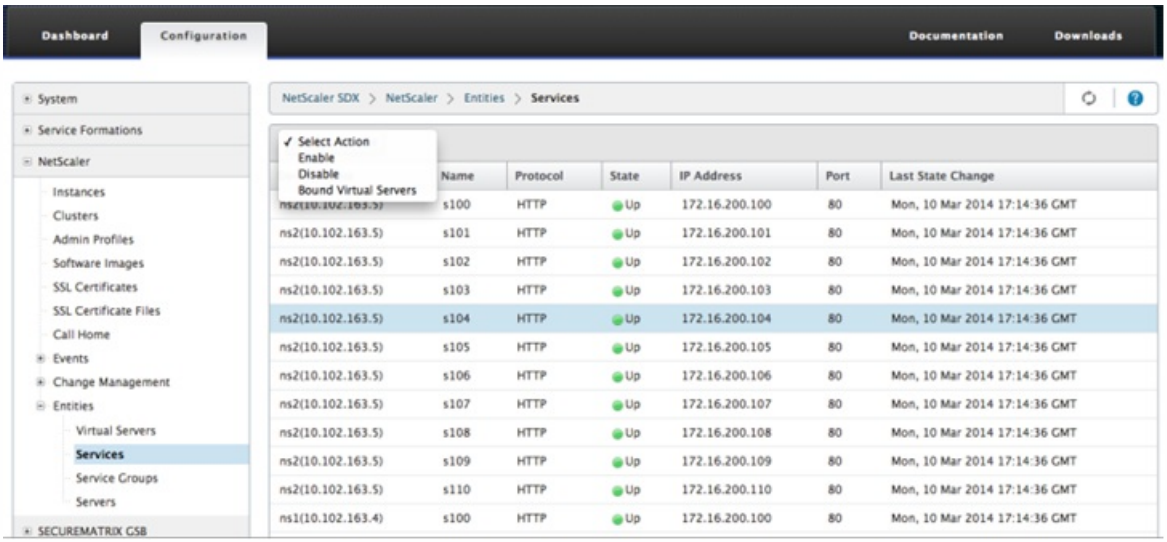
- Device Name—Name of the device on which the service is configured.
- Name—Name of the service.
- Protocol—Service type, which determines the behavior of the service. For example, HTTP, TCP, UDP, or SSL.
- State—Current state of the service. For example, UP, DOWN, or OUT OF SERVICE.
- IP Address—IP 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 Conifguration 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.



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

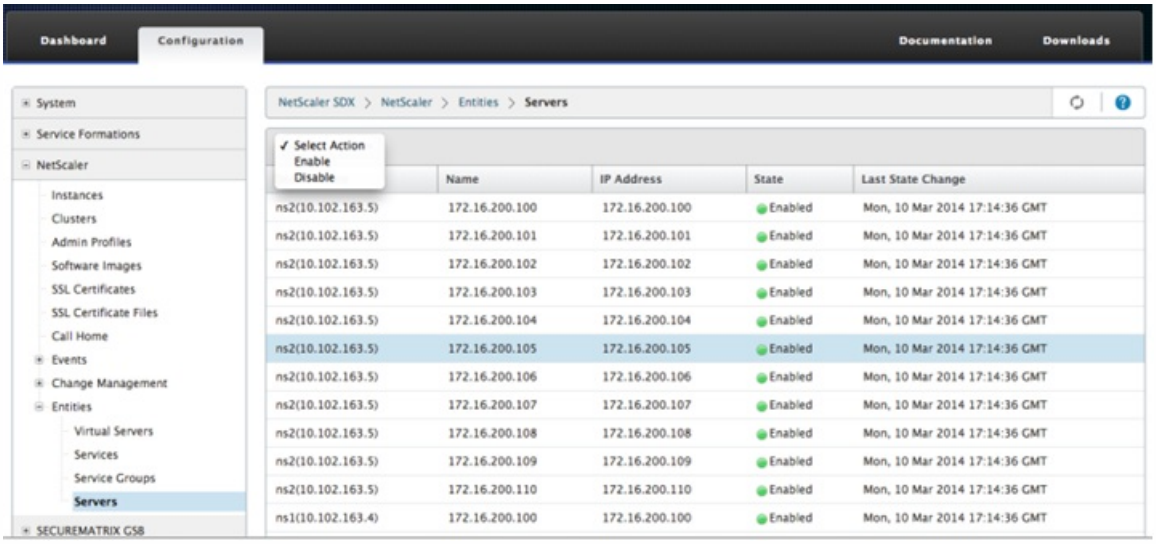
1. On the Configuration tab, in the left pane, click NetScaler > Entities > Servers.
2. In the right pane, under Servers, select the server from the list, and under Actions menu, click Bound Virtual Services. Alternately, right-click the service and click Bound Virtual Servers.

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.



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

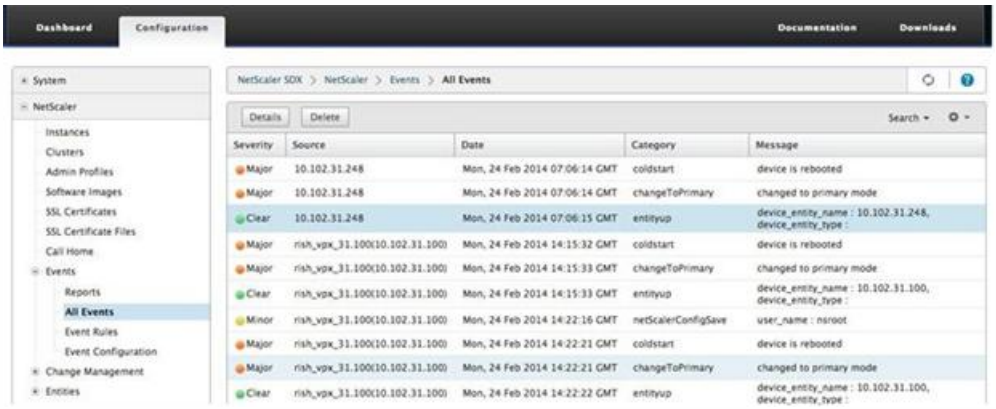
May 04, 2017

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



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.

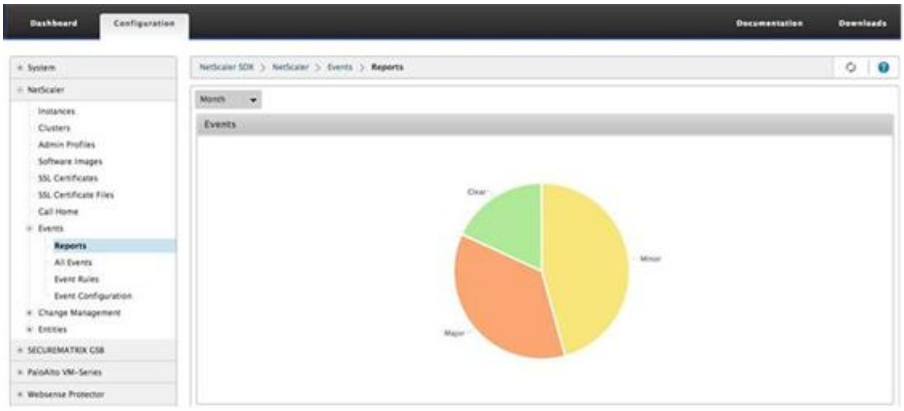
Note: After you delete the events, you will not be able to recover them.

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

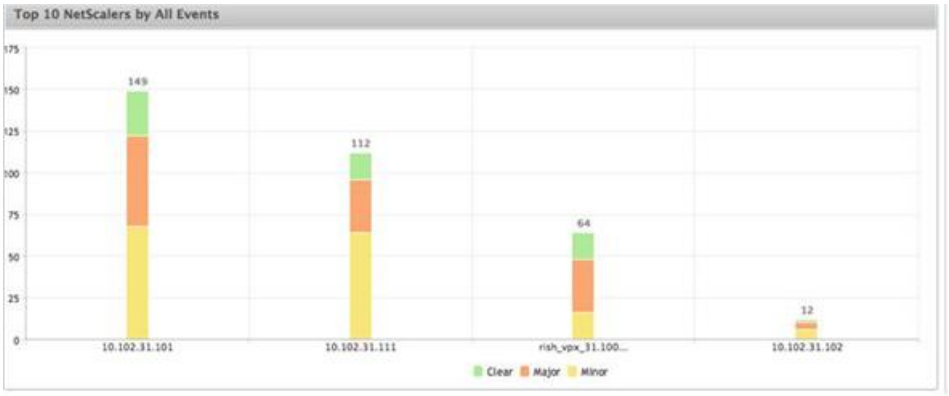
- **Events**
  The Events report is a pie chart representation of the number of events, segmented and color coded on the basis of their severity.



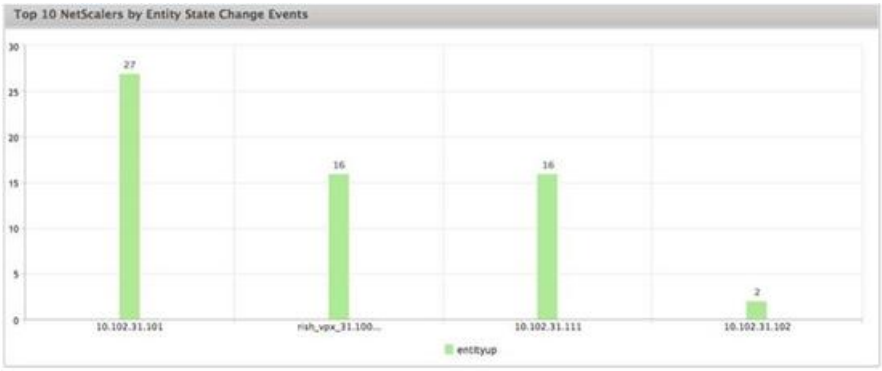
To view the details of the events of a particular severity, click that segment of the pie chart, you can view the following details:

- 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.



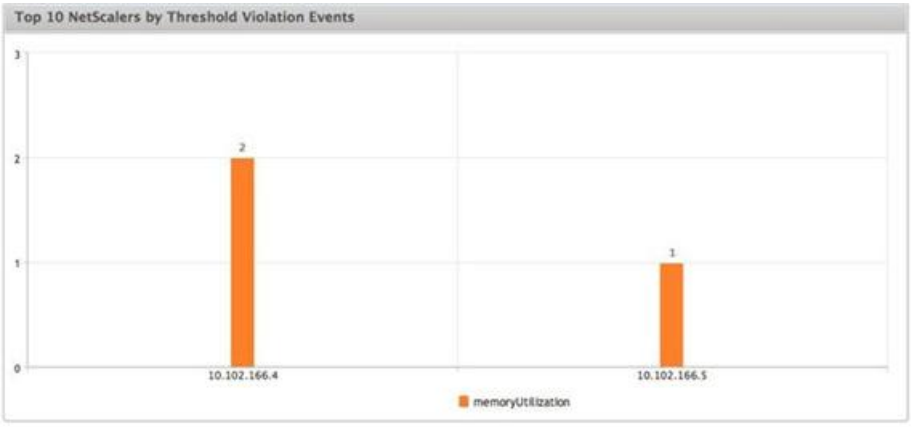
- **Top 10 NetScaler Instances by Entity State Change Events**
  This report is a bar chart that displays the top 10 NetScaler instances according to the number of entity state changes for the selected time scale. The entity state changes reflect entity up, entity down, or out of service events.



- **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:

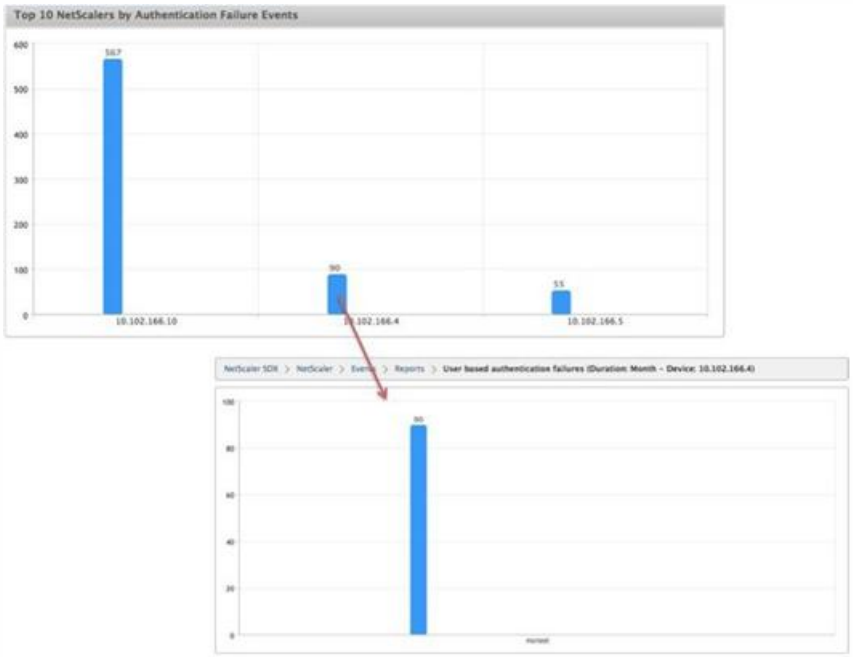
- cpuUtilization
- memoryUtilization
- diskUsageHigh
- temperatureHigh
- voltageLow
- voltageHigh
- fanSpeedLow
- temperatureCpuHigh
- interfaceThroughputLow
- interfaceBWUseHigh
- aggregateBWUseHigh



- **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

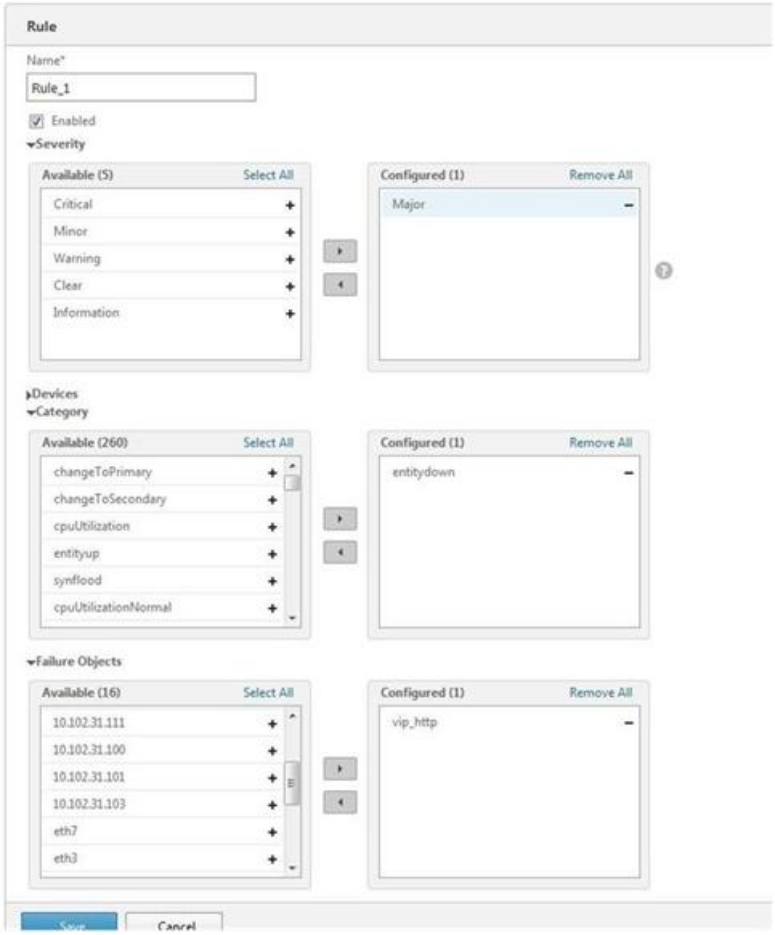
You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is executed. The conditions for which you can create filters are: severity, devices, failure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

You can assign the following actions to the events:

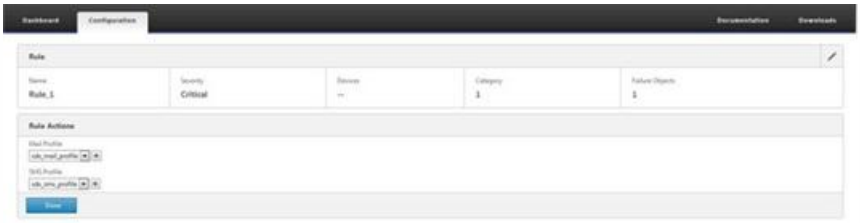
- Send e-mail Action: Sends an email for the events that match the filter criteria.
- Send SMS Action: Sends an Short Message Service(SMS) for the events that match the filter criteria.

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.



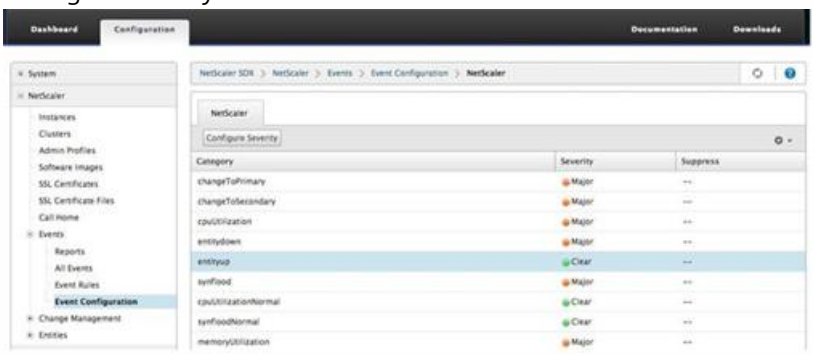
5. Click Done.

Configuring Events

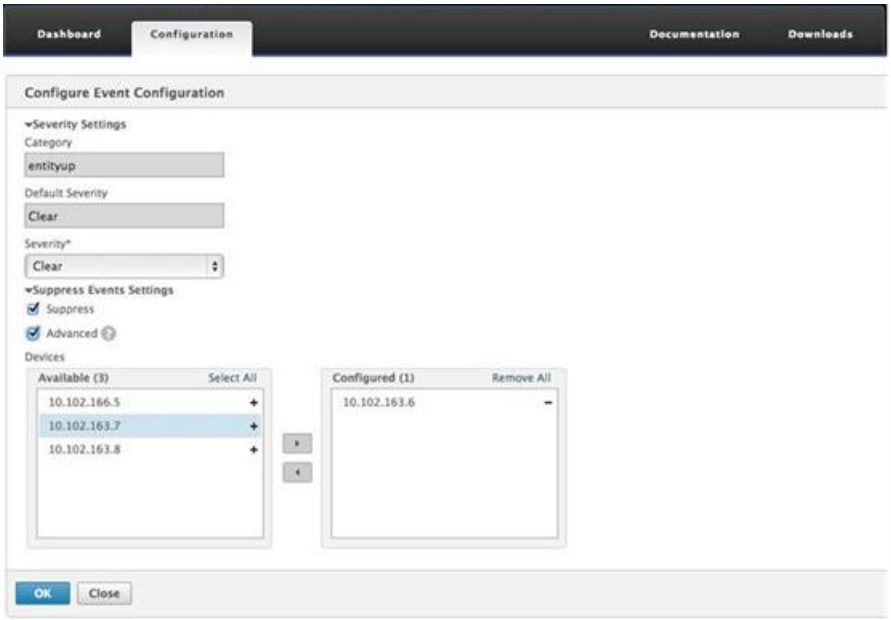
You can assign severity levels to events that are generated for the NetScaler instances on the NetScaler SDX appliance. You can define the following types of severity levels: Critical, Major, Minor, Warning, Clear, and Information. You can also suppress the events for a specific time.

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

May 04, 2017

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.

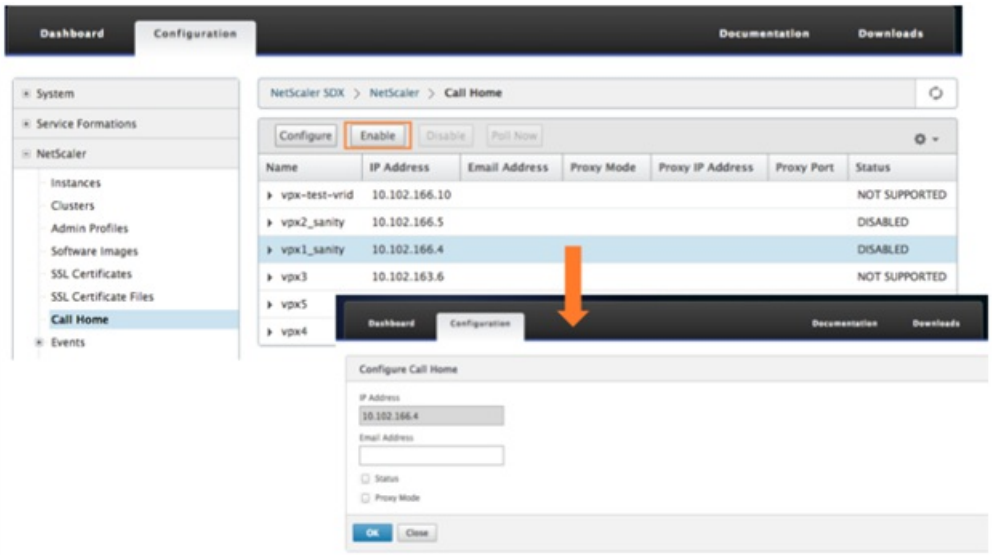
If you enable Call Home, you can configure the following options:

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.

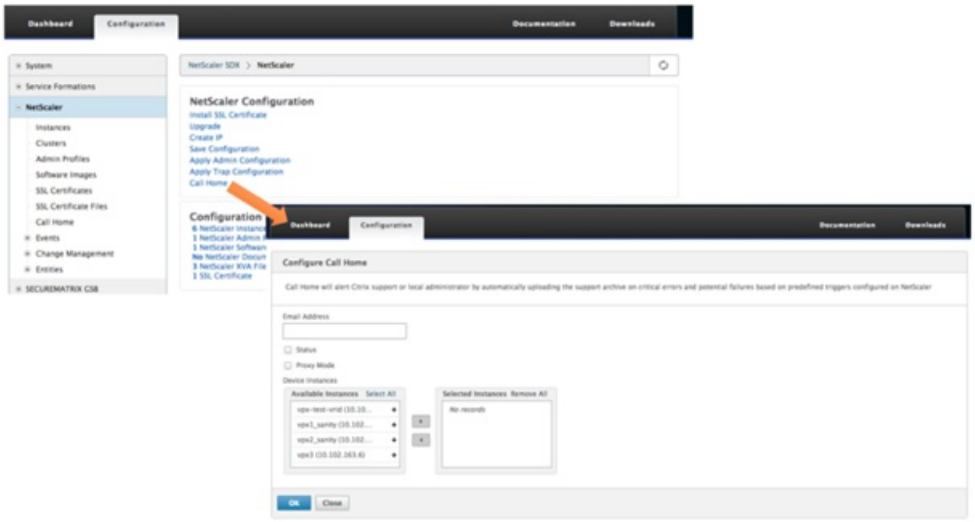
To configure Call home on the NetScaler instance from the Management Service

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

May 04, 2017

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

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

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

Monitoring the Resources on the SDX Appliance

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

Name

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

Status

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

Current Value

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

Expected Value

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

Monitoring the Storage Resources on the SDX Appliance

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

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

Name

Name of the physical disk.

Size

Size of the disk, in gigabytes (GB).

Utilized

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

Transactions/s

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

Blocks Read/s

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

Blocks Written/s

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

Total Blocks Read

Number of blocks read since the appliance was last started.

Total Blocks Written

Number of blocks written since the appliance was last started.

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

Drive Bay

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

Status

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

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

Name

System defined name of the storage depository.

Size

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

Utilized

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

Monitoring the Hardware Sensors on the SDX Appliance

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

For fan speed, the following details are displayed:

Name

Name of the fan.

Status

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

Current Value (RPM)

Current rotations per minute.

Temperature information includes the following details:

Name

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

Status

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

Current Value (Degree C)

Current temperature, in degrees, of the component.

Voltage information includes the following details:

Name

Name of the component, such as CPU core.

Status

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

Current Value (Volts)

Current voltage present on the component.

Information about the power supply includes the following details:

Name

Name of the component.

Status

State (condition) of the component. Possible values:

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

Monitoring the Interfaces on the SDX Appliance

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

Interface

Interface number on the SDX appliance.

Status

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

VFs Assigned/Total

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

Tx Packets

Number of packets transmitted since the appliance was last started.

Rx Packets

Number of packets received since the appliance was last started.

Tx Bytes

Number of bytes transmitted since the appliance was last started.

Rx Bytes

Number of bytes received since the appliance was last started.

Tx Errors

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

Rx Errors

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

Configuring the Management Service

May 04, 2017

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 20, 2016

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 admin 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 admin 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 admin 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 admin privileges, the user has admin 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, admin for a user who is to have admin 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 admin privileges else the user is assigned readonly privileges.

Adding a User Group

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.

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: admin 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

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:
     - admin—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: admin.
   - 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

Oct 04, 2016

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

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**.
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

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 ldaploginame 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.

4. Click Create, and then click Close.

Adding a TACACS Server

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 04, 2017

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 04, 2017

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.

Configuring SSL Ciphers to Securely Access the Management Service

Jan 04, 2016

You can select SSL cipher suites from a list of SSL ciphers supported by SDX appliances, and bind any combination of the SSL ciphers to access the Management Service securely through HTTPS. An SDX appliance provides 37 predefined cipher groups, which are combinations of similar ciphers, and you can create custom cipher groups from the list of supported SSL ciphers.

Limitations

- Binding ciphers with key exchange = "DH" or "ECC-DHE" is not supported.
- Binding the ciphers with Authentication = “DSS” is not supported.
- Binding ciphers that are not part of the supported SSL ciphers list, or including these ciphers in a custom cipher group, is not supported.

Supported SSL Ciphers

The following table lists the supported SSL ciphers.

Citrix Cipher Name	Openssl CipherName	Hex Code	Protocol	Key Exchange	Auth	MAC
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	SSLv3	RSA	RSA	AES(256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	SSLv3	RSA	RSA	AES(128)
TLS1.2-AES-256-SHA256	AES256-SHA256	0x003D	TLSv1.2	RSA	RSA	AES(256)
TLS1.2-AES-128-SHA256	AES128-SHA256	0x003C	TLSv1.2	RSA	RSA	AES(128)
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)
TLS1.2-AES128-GCM-SHA256	AES128-GCM-SHA256	0x009C	TLSv1.2	RSA	RSA	AES-GCM(128)
TLS1-ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	0xC014	SSLv3	ECC-DHE	RSA	AES(256)
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	SSLv3	ECC-DHE	RSA	AES(128)

TLS1.2-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	0xC028	TLSv1.2	ECC-DHE	RSA	AES(256)
TLS1.2-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	0xC027	TLSv1.2	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	0xC02F	TLSv1.2	ECC-DHE	RSA	AES-GCM(128)
TLS1.2-DHE-RSA-AES-256-SHA256	DHE-RSA-AES256-SHA256	0x006B	TLSv1.2	DH	RSA	AES(256)
TLS1.2-DHE-RSA-AES-128-SHA256	DHE-RSA-AES128-SHA256	0x0067	TLSv1.2	DH	RSA	AES(128)
TLS1.2-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	0x009F	TLSv1.2	DH	RSA	AES-GCM(256)
TLS1.2-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	0x009E	TLSv1.2	DH	RSA	AES-GCM(128)
TLS1-DHE-RSA-AES-256-CBC-SHA	DHE-RSA-AES256-SHA	0x0039	SSLv3	DH	RSA	AES(256)
TLS1-DHE-RSA-AES-128-CBC-SHA	DHE-RSA-AES128-SHA	0x0033	SSLv3	DH	RSA	AES(128)
TLS1-DHE-DSS-AES-256-CBC-SHA	DHE-DSS-AES256-SHA	0x0038	SSLv3	DH	DSS	AES(256)
TLS1-DHE-DSS-AES-128-CBC-SHA	DHE-DSS-AES128-SHA	0x0032	SSLv3	DH	DSS	AES(128)
TLS1-ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA	0xC012	SSLv3	ECC-DHE	RSA	3DES(168)
SSL3-EDH-RSA-DES-	EDH-RSA-DES-CBC3-	0x0016	SSLv3	DH	RSA	3DES(168)

CBC3-SHA	SHA					
SSL3-EDH-DSS-DES-CBC3-SHA	EDH-DSS-DES-CBC3-SHA	0x0013	SSLv3	DH	DSS	3DES(168)
TLS1-ECDHE-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA	0xC011	SSLv3	ECC-DHE	RSA	RC4(128)
SSL3-DES-CBC3-SHA	DES-CBC3-SHA	0x000A	SSLv3	RSA	RSA	3DES(168)
SSL3-RC4-SHA	RC4-SHA	0x0005	SSLv3	RSA	RSA	RC4(128)
SSL3-RC4-MD5	RC4-MD5	0x0004	SSLv3	RSA	RSA	RC4(128)
SSL3-DES-CBC-SHA	DES-CBC-SHA	0x0009	SSLv3	RSA	RSA	DES(56)
SSL3-EXP-RC4-MD5	EXP-RC4-MD5	0x0003	SSLv3	RSA(512)	RSA	RC4(40)
SSL3-EXP-DES-CBC-SHA	EXP-DES-CBC-SHA	0x0008	SSLv3	RSA(512)	RSA	DES(40)
SSL3-EXP-RC2-CBC-MD5	EXP-RC2-CBC-MD5	0x0006	SSLv3	RSA(512)	RSA	RC2(40)
SSL2-DES-CBC-MD5	DHE-DSS-AES128-SHA256	0x0040	SSLv2	RSA	RSA	DES(56)
SSL3-EDH-DSS-DES-CBC-SHA	EDH-DSS-DES-CBC-SHA	0x0012	SSLv3	DH	DSS	DES(56)
SSL3-EXP-EDH-DSS-DES-CBC-SHA	EXP-EDH-DSS-DES-CBC-SHA	0x0011	SSLv3	DH(512)	DSS	DES(40)
SSL3-EDH-RSA-DES-CBC-SHA	EDH-RSA-DES-CBC-SHA	0x0015	SSLv3	DH	RSA	DES(56)
SSL3-EXP-EDH-RSA-DES-CBC-SHA	EXP-EDH-RSA-DES-CBC-SHA	0x0014	SSLv3	DH(512)	RSA	DES(40)
SSL3-ADH-RC4-MD5	ADH-RC4-MD5	0x0018	SSLv3	DH	None	RC4(128)

SSL3-ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	0x001B	SSLv3	DH	None	3DES(168)
SSL3-ADH-DES-CBC-SHA	ADH-DES-CBC-SHA	0x001A	SSLv3	DH	None	DES(56)
TLS1-ADH-AES-128-CBC-SHA	ADH-AES128-SHA	0x0034	SSLv3	DH	None	AES(128)
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLv3	DH	None	AES(256)
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLv3	DH(512)	None	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLv3	DH(512)	None	DES(40)
SSL3-NULL-MD5	NULL-MD5	0x0001	SSLv3	RSA	RSA	None
SSL3-NULL-SHA	NULL-SHA	0x0002	SSLv3	RSA	RSA	None

Predefined Cipher Groups

The following table lists the predefined cipher groups provided by the SDX appliance.

Cipher Group Name	Description
ALL	All ciphers supported by NetScaler excluding NULL ciphers
DEFAULT	Default cipher list with encryption strength >= 128bit
kRSA	Ciphers with Key-ex algo as RSA
kEDH	Ciphers with Key-ex algo as Ephemeral-DH
DH	Ciphers with Key-ex algo as DH
EDH	Ciphers with Key-ex/Auth algo as DH
aRSA	Ciphers with Auth algo as RSA
aDSS	Ciphers with Auth algo as DSS

Cipher Group Name	Description
DSS	Ciphers with Auth algo as DSS
DES	Ciphers with Enc algo as DES
3DES	Ciphers with Enc algo as 3DES
RC4	Ciphers with Enc algo as RC4
RC2	Ciphers with Enc algo as RC2
eNULL	Ciphers with Enc algo as NULL
MD5	Ciphers with MAC algo as MD5
SHA1	Ciphers with MAC algo as SHA-1
SHA	Ciphers with MAC algo as SHA
NULL	Ciphers with Enc algo as NULL
RSA	Ciphers with Key-ex/Auth algo as RSA
ADH	Ciphers with Key-ex algo as DH and Auth algo as NULL
SSLv2	SSLv2 protocol ciphers
SSLv3	SSLv3 protocol ciphers
TLSv1	SSLv3/TLSv1 protocol ciphers
TLSv1_ONLY	TLSv1 protocol ciphers
EXP	Export ciphers
EXPORT	Export ciphers
EXPORT40	Export ciphers with 40bit encryption
EXPORT56	Export ciphers with 56bit encryption
LOW	Low strength ciphers (56bit encryption)
MEDIUM	Medium strength ciphers (128bit encryption)
HIGH	High strength ciphers (168bit encryption)
AES	AES Ciphers
FIPS	FIPS Approved Ciphers

Cipher Group Name	Description
AES-GCM	Ciphers with Enc algo as AES-GCM
SHA2	Ciphers with MAC algo as SHA-2

Viewing the Predefined Cipher Groups

To view the predefined cipher groups, on the **Configuration** tab, in the navigation pane, expand **Management Service**, and then click **Cipher Groups**.

Creating Custom Cipher Groups

You can create custom cipher groups from the list of supported SSL ciphers.

To create custom cipher groups:

1. On the **Configuration** tab, in the navigation pane, expand **Management Service**, and then click **Cipher Groups**.
2. In the **Cipher Groups** pane, click **Add**.
3. In the **Create Cipher Group** dialog box, perform the following:
   1. In the **Group Name** field, enter a name for the custom cipher group.
   2. In the **Cipher Group Description** field, enter a brief description of the custom cipher group.
   3. In the **Cipher Suites** section, click **Add** and select the ciphers to include in the list of supported SSL ciphers.
   4. Click **Create**.

Viewing Existing SSL Cipher Bindings

To view the existing cipher bindings, on the **Configuration** tab, in the navigation pane, expand **System**, and then click **Change SSL Settings** under **System Settings**.

> **Note**
>
> After you upgrade to the latest version of the Management Service, the list of existing cipher suites shows the OpenSSL names. Once you bind the ciphers from the upgraded Management Service, the display uses the Citrix naming convention.

Binding Ciphers to the HTTPS Service

To bind ciphers to the HTTPS service:

1. On the **Configuration** tab, in the navigation pane, click **System**.
2. In the **System** pane, under System Settings, click **Change SSL Settings**.
3. In the **Edit Settings** pane, click **Ciphers Suites**.
4. In the **Ciphers Suites** pane, do either of the following:
   - To choose cipher groups from predefined cipher groups provided by SDX appliance, select the **Cipher Groups** check box, select the cipher group from the **Cipher Groups** drop-down list, and then click **OK**.
   - To choose from the list of supported ciphers, select the **Cipher Suites** check box, click **Add** to select the ciphers, and then click **OK**.

Backing Up and Restoring the Configuration Data of the SDX Appliance

Oct 20, 2016

The NetScaler SDX appliance backup process is a single step process that creates a backup file containing the following:

- Single bundle image:
  - XenServer image
  - Hotfixes and Supplemental Packs of XenServer
  - Management Service image
- NetScaler XVA image
- NetScaler upgrade image
- Management Service configuration
- NetScaler SDX configuration
- NetScaler configuration

From release 11.0.64.x onwards, you can encrypt the backup files using a password to ensure that the backup file is secure.

To backup the current configuration:

1. On the **Configuration** tab, in the navigation pane, expand **Management Service**, and then click **Backup Files**.
2. In the **Backup Files** pane, click **Back Up**.
3. in the **New Backup File** dialog box, select the **Password Protect file** check box to encrypt the backup file.
4. In the **Password** and **Confirm Password** fields, enter and confirm the password for the backup file.
5. Click **Continue**.

The backup process creates a backup file and the filename of the backup file inculdes the current IP address of the Management Service and the timestamp when the backup was taken.

Scheduled Backup

By default, NetScaler SDX creates a backup every 24 hours using a backup policy. Using the backup policy, you can define the number of backup files that you want to retain in the SDX appliance and also you can encrypt the scheduled backup files using a password to ensure that the backup file is secure.

To edit the backup policy:

1. On the **Configuration** tab, click **System**.
2. In the **Policy Administration** pane, click **Backup Policy**.
3. In the **Configure backup policy** pane, perform the following:
   1. In the **Previous backups to retain** field, enter the number of backup files you want to retain.
   2. To encrypt the backup files, select **Encrypt Backup File** check box.
   3. In the **Password** and **Confirm Password** fields, enter and confirm the password to encrypt the backup file.

Manually Transfer the Backup File to a External Backup Server

You can manually transfer the backup file to an external backup server. Make sure that you have the external backup server details before you manually transfer the backup file.

To manually transfer the backup file to an external backup server:

1. On the **Configuration** tab, in the navigation pane, expand **Management Service**, and then click **Backup Files**.
2. In the **Backup Files** pane, select the backup file and then click **Transfer**.
3. In the **Server** field, enter hostname or IP address of the external backup server.
4. In the **User Name** and **Password** fields, enter the username and password to access the external backup server.
5. In the **Port** field, enter the port number.
6. In the **Transfer Protocol** field, select the protocol you want to use to transfer the backup file to the external backup server.
7. In the **Directory Path** field, enter the path of the directory in the external backup server where you want to store the backup files.
8. Select **Delete file from Management Service** after transfer if you want to delete the backup file from the SDX appliance after you have transfered the backup file to the external backup server.
9. Click **OK**.

Restoring the Appliance

You can restore the NetScaler SDX appliance to the configuration available in the backup file. During the appliance restore, all the current configuration is deleted.

> **Note**
>
> If you are restoring the NetScaler SDX appliance using the backup of a different NetScaler SDX appliance, make sure that you add the licenses and configure Management Service network settings in the appliance as per the settings available in the backup file before you start the restore process.
>
> Make sure that the platform variant on which the backup was taken is same as on which you are trying to restore (restoring the backup's between different platform variants is not supported).

To restore the appliance from the backup file:

1. On the **Configuration** tab, in the navigation pane, expand **Management Service**, and then click **Backup Files**.
2. In the **Backup Files** pane, select the backup file and then click **Restore**.
3. In the **Restore** dialog box, select **Appliance Restore**, and then click **OK**.
4. (Optional) If the backup file is encrypted, when prompted, enter the password and then click **OK**.

Restoring the NetScaler instance

You can restore the NetScaler instance in the NetScaler SDX appliance to the NetScaler instances that are available in the backup file.

To restore the NetScaler instance in the backup file:

1. On the **Configuration** tab, in the navigation pane, expand **Management Service**, and then click **Backup Files**.
2. In the **Backup Files** pane, select the backup file and then click **Restore**.
3. In the **Restore** dialog box, select **Instance Restore**.
4. Select the NetScaler instances that you want to restore and then click **OK**.
5. (Optional) If the backup file is encrypted, when prompted, enter the password and then click **OK**.

Performing Appliance Reset

Aug 08, 2017

NetScaler SDX appliance allows you to:

- Reset the configuration of the Appliance.
- Reset the Appliance to factory version
- Reset the Appliance to a particular Single Bundle Image version

Before performing an appliance 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 an appliance 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.

The Management Service provides the Config Reset option to reset the configuration of the Appliance. The Config Reset option performs the following:

- 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.

> ### Important
>
> When you factory reset the appliance, it defaults back to the factory version.

Performing Factory Reset by Using NetScaler GUI

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. On the NetScaler GUI, click Configuration > System > Sytem Administration > Appliance Reset.
2. In the Appliance Reset dialog box, select the reset type from the drop-down list.
3. Click OK.

For more information about how to perform different reset types, see the details provided in NetScaler 11.1 documentation.

Provisioning NetScaler Instances

Oct 20, 2016

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.

> ### Warning
>
> Make sure that you modify the provisioned network interfaces or VLANS of an instance using the Management Service instead of performing the modifications directly on the instance.

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.

Nexthop*
The alternate IP address for the static route in VPX that should be used to establish connection with the Management Service, if the default route is not available.

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.

Managing Crypto Capacity

Jul 30, 2018

Starting with release 11.0 72.xx, the interface to manage crypto capacity has changed. With the new interface, the Management Service provides asymmetric crypto units (ACUs), symmetric crypto units (SCUs), and crypto virtual interfaces to represent SSL capacity on the NetScaler SDX appliance. Earlier crypto capacity was assigned in units of SSL chips, SSL cores, and SSL virtual functions. See the Legacy SSL chips to ACU/SCU conversion table for more information about how legacy SSL chips translate into ACU and SCU units.

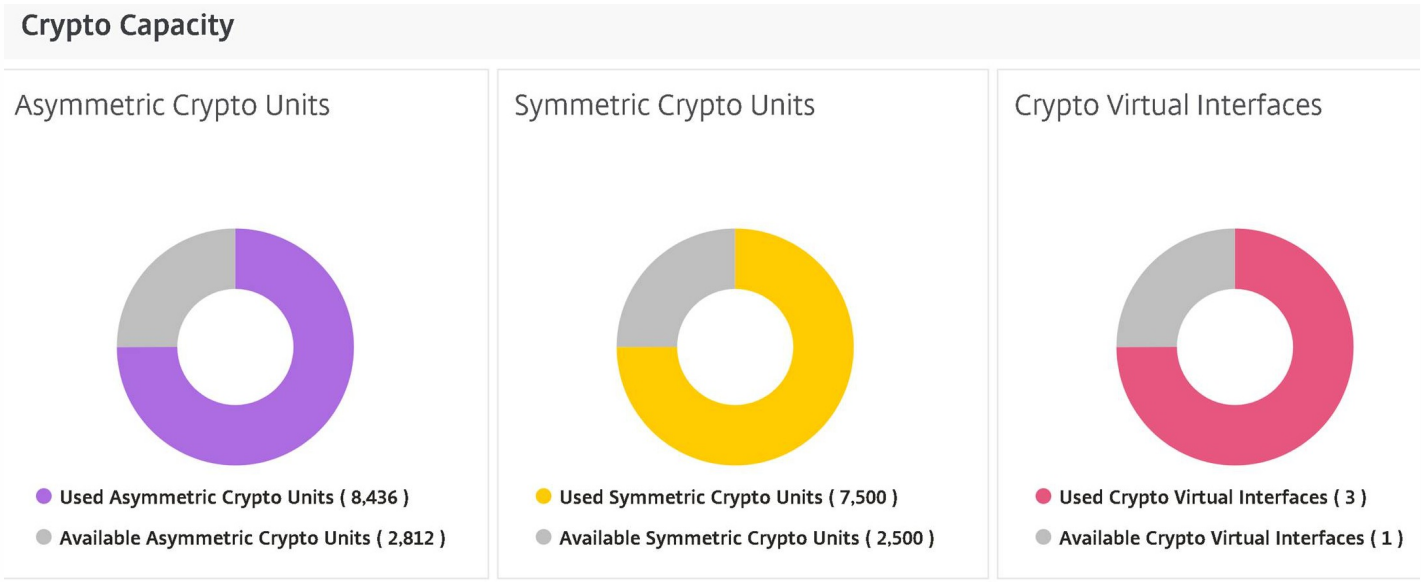
By using the Management Service GUI, you can allocate crypto capacity to the NetScaler VPX instance in units of ACU and SCU.

The following table provides brief descriptions about ACUs, SCUs, and crypto virtual instances.

Crypto Units	Description
Asymmetric Crypto Unit (ACU)	1 ACU = 1 operation per second (ops) of (RSA) 2 K (2048-bit key size) decryption. For further details, refer to the ACU to PKE resource conversion table.
Symmetric Crypto Unit (SCU)	1 SCU = 1 Mbps of AES-128-CBC + SHA256-HMAC @ 1024 B This definition is applicable for all SDX platforms.
Crypto Virtual Interfaces	Also known as virtual functions, crypto virtual interfaces represent the basic unit of the SSL hardware. After these interfaces are exhausted, the SSL hardware cannot be further assigned to a NetScaler VPX instance. Crypto virtual interfaces are read-only entities, and the NetScaler SDX appliance automatically allocates these entities.

View Crypto Capacity

You can view the crypto capacity of the SDX appliance in the dashboard of the NetScaler SDX GUI. The dashboard displays the used and available ACUs, SCUs, and virtual interfaces on the NetScaler SDX appliance. To view the crypto capacity, navigate to **Dashboard > Crypto Capacity**.



Allocate Crypto Capacity While Provisioning the NetScaler VPX Instance

While provisioning a NetScaler VPX instance on NetScaler SDX, in the Crypto Allocation section, you can allocate the number of ACUs and SCUs for the NetScaler VPX instance. For instructions to provision a NetScaler VPX instance, see Provisioning NetScaler Instances.

To allocate crypto capacity while provisioning a NetScaler VPX instance:

1. Log on to the Management Service.

2. Navigate to **Configuration > NetScaler > Instances**, and click **Add.**

3. In the **Crypto Allocation** section, you can view the available ACUs, SCU, and crypto virtual interfaces. The way to allocate ACUs and SCUs differs depending on the SDX appliance:

    a. For the appliances listed in the Minimum value of an ACU counter available for different SDX appliances table, you can assign ACUs in multiples of a specified number. SCUs are automatically allocated and the SCU allocation field is not editable. You can increase ACU allocation in the multiples of the minimum ACU available for that model. For example, if minimum ACU is 4375, subsequent ACU increment is 8750, 13125, and so on.

Example. Crypto allocation where SCUs are automatically assigned and ACUs are assigned in multiples of a number specified in the following table, for respective SDX appliances.

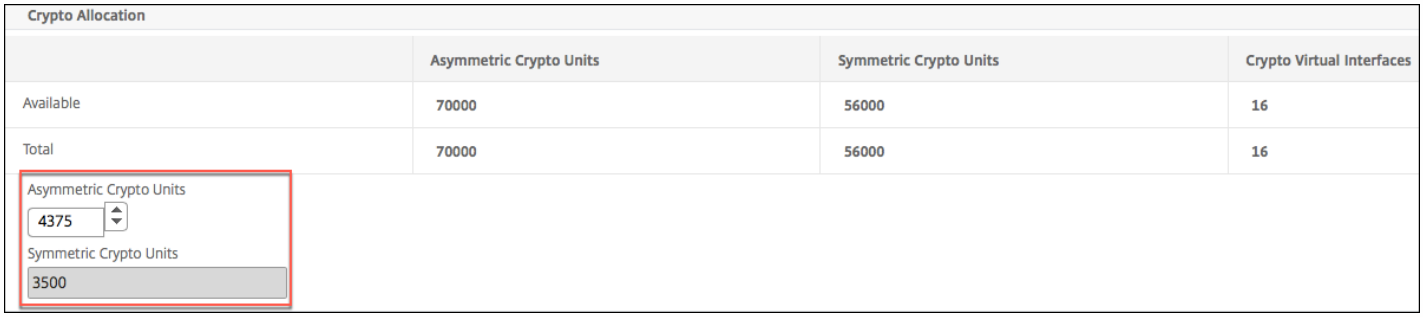
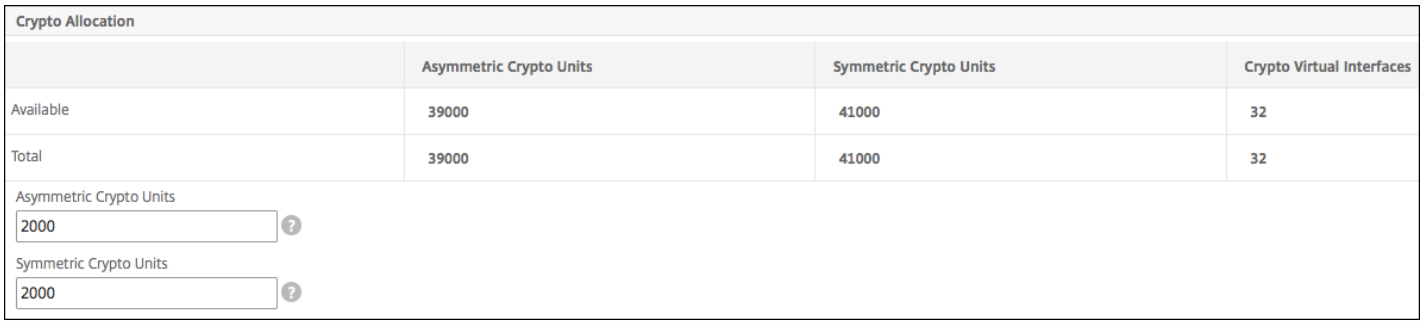


Table. Minimum value of an ACU counter available for different SDX appliances

NetScaler SDX platform	ACU counter minimum value
• 22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ports)	2187
• 8400, 8600, 8010, 8015 • 17500, 19500, 21500 • 17550, 19550, 20550, 21550 • 11500, 13500, 14500, 16500, 18500, 20500	2812
• 11515, 11520, 11530, 11540, 11542 • 14xxx • 14xxx 40S • 14xxx 40G • 14xxx FIPS • 25xxx • 25xxx A	4375

b. For the rest of the SDX platforms, which are not listed on the above Minimum value of an ACU counter available for different SDX appliances table, you can freely assign ACUs and SCUs. The NetScaler SDX appliance automatically allocates crypto virtual interfaces.

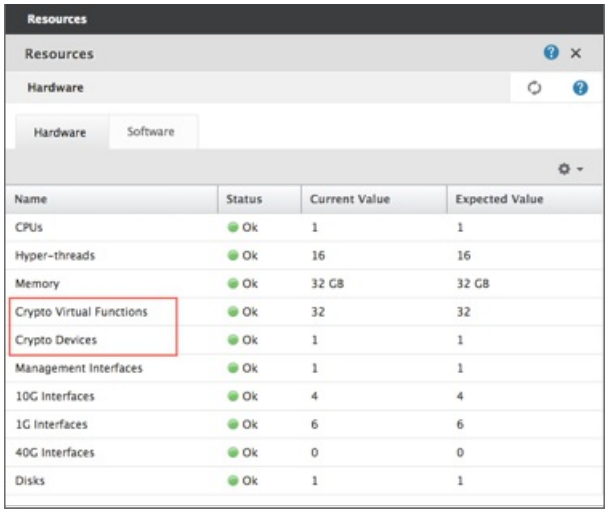
Example. Crypto allocation where both ACU and SCUs are freely assigned



4. Complete all the steps for provisioning the NetScaler instance, and click **Done**. For more information, see Provisioning NetScaler Instances.

Viewing the Health of the Crypto Hardware

In Management Service, you can view the health of the crypto hardware provided with the NetScaler SDX. The health of the crypto hardware is represented as Crypto Devices and Crypto Virtual Functions. To view the health of the crypto hardware, navigate to **Dashboard > Resources**.



Points to Note

Keep the following points in mind when you upgrade the NetScaler SDX appliance to 12.0 57.xx and higher versions.

- Only the SDX user interface gets upgraded, but the hardware capacity of the appliance remains the same.
- The crypto allocation mechanism remains the same, and only the representation on SDX GUI changes.
- Crypto interface is backward compatible, and it does not affect any existing automation mechanism that uses NITRO interface to manage the SDX appliance.
- Upon SDX appliance upgrade, the crypto assigned to the existing VPX instances does not change; only its representation on Management Service changes.

Table: ACU to PKE resource conversion

NetScaler SDX platform	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ports)	2187	12497	2187	312	256	190
8400, 8600, 8010, 8015	2812	17000	2812	424	330	N/A
11515, 11520, 11530, 11540, 11542	4375	25000	4375	625	512	381
22040, 22060, 22080,22100, 22120 (24 ports)	4375	25000	4375	625	512	381
17500, 19500, 21500	2812	17000	2812	424	330	N/A
17550, 19550, 20550, 21550	2812	17000	2812	424	330	N/A
11500, 13500, 14500, 16500, 18500, 20500	2812	17000	2812	424	330	N/A
14xxx, 14xxx 40G, 25xxx, 25xxx A	4375	25000	4375	625	512	381
14xxx FIPS	4375	25000	4375	625	512	381
14xxx 40S	4375	25000	4375	625	512	381
*26xxx	1000	4615	1000	136	397	4949
*15000 50G	1000	4615	1000	136	397	4949

* On these platforms the PKE numbers are minimum guaranteed values.

How to read the ACU to PKE resource conversion table

The ACU to PKE resource conversion table is based on the following points:

- Management Service helps allocate Crypto Resources to each individual VPX. Management Service cannot allocate or promise performance.
- Actual performance varies depending on packet size, cipher/Keyex/HMAC (or their variations) used, and so on

The following example helps you understand how to read and apply the ACU to PKE resource conversion table.

Example: ACU to PKE resource conversion for the SDX 22040 platform

Allocation of 2187 ACUs to a Netscaler VPX instance on an SDX 22040 platform allocates crypto resource equivalent to 256 ECDHE-RSA operations or 2187 RSA-2K operations and so on.

Table: Legacy SSL chips to ACU/SCU conversion

	Before upgrade	After upgrade		

NetScaler SDX platform	Total SSL chips (As seen from Management Service, before upgrade.)	Total ACU	Total SCU	ACU/SCU equivalent to one SSL chip (Multiplier used for allocation)
22040, 22060, 22080,22100, 22120 (24 ports)	128	560000	448000	4375/3500
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ports)	64	139968	112000	2187/1750
14xxx 40S	64	280000	224000	4375/3500
17550, 19550, 20550, 21550	36	101232	90000	2812/2500
14xxx, 14xxx 40G, 25xxx, 25xxx A	32	140000	112000	4375/3500
11515, 11520, 11530, 11540, 11542	16	70000	56000	4375/3500
17500, 19500, 21500	16	44992	40000	2812/2500
11500, 13500, 14500, 16500, 18500, 20500	16	44992	40000	2812/2500
14xxx FIPS	8	35000	28000	4375/3500
8400, 8600, 8010, 8015	4	11248	10000	2812/2500
***26xxx**	NA	39000	41000	N/A
***15000 50G**	N/A	39000	41000	N/A

Bandwidth Metering in NetScaler SDX

Oct 05, 2016

SDX bandwidth metering provides you with an accurate, reliable and easy to use metering scheme that lets you to efficiently allocate processing capacity and monetize bandwidth usage in simple and accurate manner. A metering scheme is required to optimally allocate the bandwidth among various resources, keeping in mind that all the users at all the times get the allocated bandwidth.

The bandwidth allocation can be done in the following two modes:

- Dedicated bandwidth with a fixed rate of throughput
- Dedicated bandwidth with minimum assured throughput and bandwidth bursting ability

Dedicated bandwidth with a fixed rate of throughput

In this bandwidth allocation method, each VPX is assigned a dedicated bandwidth. The VPX is allowed to use the bandwidth up to the limit set. In dedicated mode the minimum and maximum bandwidth allocated are the same. If during a period of time, the VPX requires more bandwidth than allocated, then in the dedicated mode the VPX cannot increase its throughput. This can be a downside if a VPX is serving critical requests.

Also, if an SDX appliance has a number of VPXs and few of them are not utilizing their allocated bandwidth, then in dedicated mode it is not possible to share their unused bandwidth. To overcome all these challenges, a dedicated bandwidth with minimum assured rate with the ability to dynamically increase the bandwidth is useful.

Dedicated bandwidth with minimum assured throughput and bandwidth bursting ability

In this bandwidth allocation method, a VPX is allocated a minimum assured bandwidth with the flexibility to increase its bandwidth up to a preset limit. The extra bandwidth that a VPX can use is called burst capacity.

The benefit of burst capacity is that if some of VPXs are having extra capacity which they are not using, then that can be allocated to other VPX which are fully utilizing their allocated bandwidth and require more for certain periods of time. Various service providers are also interested in providing various add-on services to their customers that require dedicated capacity. At the same time they do not want to over provision bandwidth. Burstable bandwidth helps in such scenarios where the customers are assured of a specific bandwidth with the option to increase the bandwidth during high demand periods.

Selecting the Bandwidth Allocation Mode

Before you choose burstable throughput, you need to enable dynamic burst throughput allocation. To enable this option, navigate to Configuration > System and from the System Settings group, select Change System Settings. Click on the Enable Dynamic Burst Throughput Allocation check box to enable dynamic throughput.

When you provision a VPX, you can select from bandwidth burst or dynamic throughput. In the SDX UI, click Configuration > NetScaler > Instances > Add. In the Resource Allocation section of the Provision NetScaler page, choose Burstable option from the Throughput Allocation Mode drop down list for burstable throughput. If you want to use fixed rate of throughput, select Fixed. By default, fixed mode is set for bandwidth allocation. It is not necessary that all the VPXs work in the same mode. Each VPX can be configured in different mode.

Note: If you are migrating SDX from a release prior to 10.5.e, then by default all the VPXs are in the fixed allocation mode.

Determining the Maximum Burst Bandwidth for a VPX instance

Updated: 2014-10-14

The extent to which each VPX is allowed to burst is computed through an algorithm. When you provision a VPX with burstable bandwidth, then each such VPX has to be given a priority. The allocation of burstable bandwidth depends on this burst priority. The priority varies from P0 to P4 with P0 being the highest priority and P4 being the lowest.

Let us take a case where there are 2 VPX, namely VPX1 and VPX2. The minimum bandwidth allocated to VPX1 and VPX2 are 4Gbps and 2Gbps respectively with a burstable bandwidth of 2Gbps and 1Gbps each. The following table depicts the parameters:

VPX Name	Parameter	Value
VPX1	Minimum assured bandwidth	4Gbps
	Maximum Burstable bandwidth	2Gbps
	Priority	P0
VPX2	Minimum assured bandwidth	2Gbps
	Maximum Burstable bandwidth	1Gbps
	Priority	P1

In the above case, let us assume that the total licensed bandwidth is 8 Gbps. Now, if both the VPX are bursting to their maximum burstable limit, that is:

1. VPX1 is using its maximum burstable bandwidth, that is 2 Gpbs then it is using a total of 4 + 2 = 6 Gbps
2. VPX2 is using its maximum burstable bandwidth, that is 1 Gpbs then it is using a total of 2 + 1 = 3 Gbps

In this case the maximum bandwidth that is used is more than the licensed capacity of 8 Gbps. So to bring down the usage to within the licensed capacity, one of the VPX would have to give up its burstable bandwidth. In this case since VPX2 has lower priority than VPX1, so it gives up its 1 Gbps burstable bandwidth. VPX1 would continue to burst as it has higher priority than VPX2. In all such scenarios, it is made sure that the minimum guaranteed bandwidth is always honored.

Checking the throughput and data consumption statistics

Updated: 2014-10-14

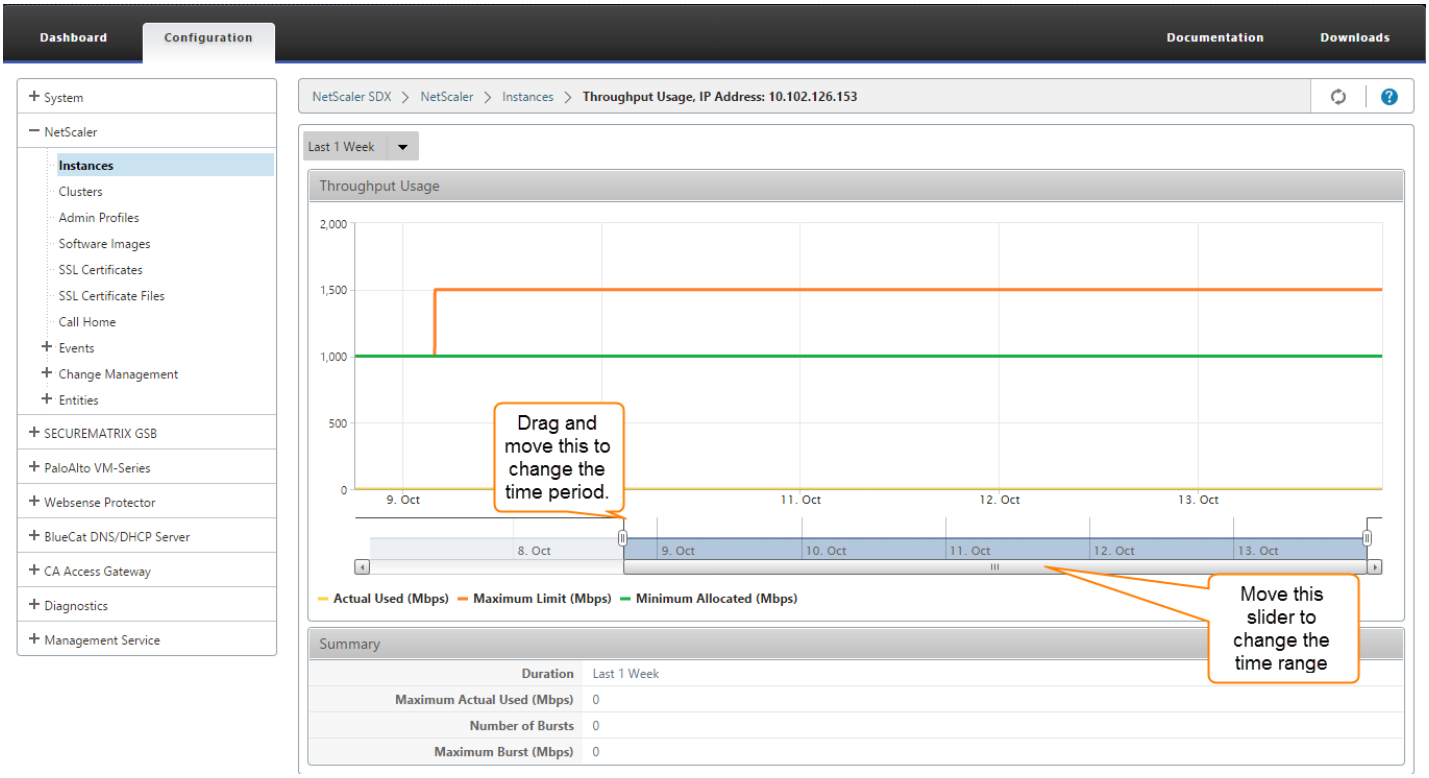
You can check individual VPX's throughput and data consumption statistics in graphs. These graphs are accessible from the Configuration > NetScaler > Instances page. Select a VPX and then click on the Action drop list. From the list select either Througput Statistics or Data Usage Statistics.

The graphs provide you to check the data consumption and throughput statistics for various periods of time, like:

- Last 1 hour
- Last 1 day
- Last 1 week
- Last 1 month, and
- Previous month

You can also select a specific time period in the graph by adjusting the slider at the bottom of the graph. The graph also shows the data consumption or throughput data for a specific time by moving your mouse over the lines in the graph.

The following illustration shows a sample graph of throughput data for 1 week:



Setting up a Cluster of NetScaler Instances

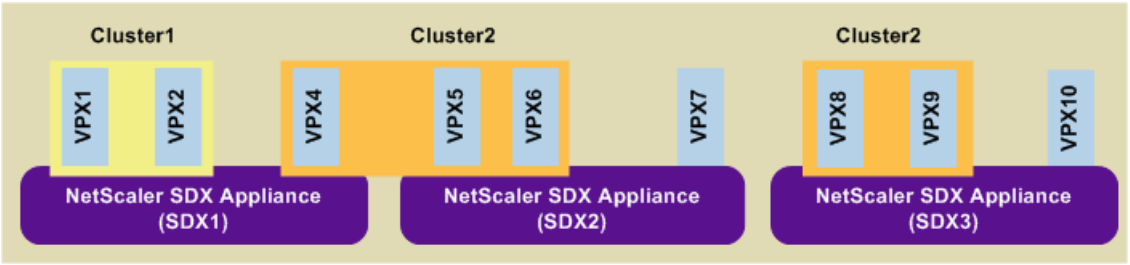
Jul 18, 2017

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.
- From NetScaler 10.5 onwards, jumbo frames are not supported on a NetScaler cluster that is made up of NetScaler SDX instances.

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

Oct 20, 2016

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.

> ### Warning
>
> Make sure that you modify the provisioned network interfaces or VLANS of an instance using the Management Service instead of performing the modifications directly on the instance.

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

May 04, 2017

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

May 04, 2017

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.

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

May 04, 2017

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.

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

May 04, 2017

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.

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.

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.

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

May 04, 2017

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.

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.

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.

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.

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.

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

May 04, 2017

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.

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.

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.

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.

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.

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

May 04, 2017

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

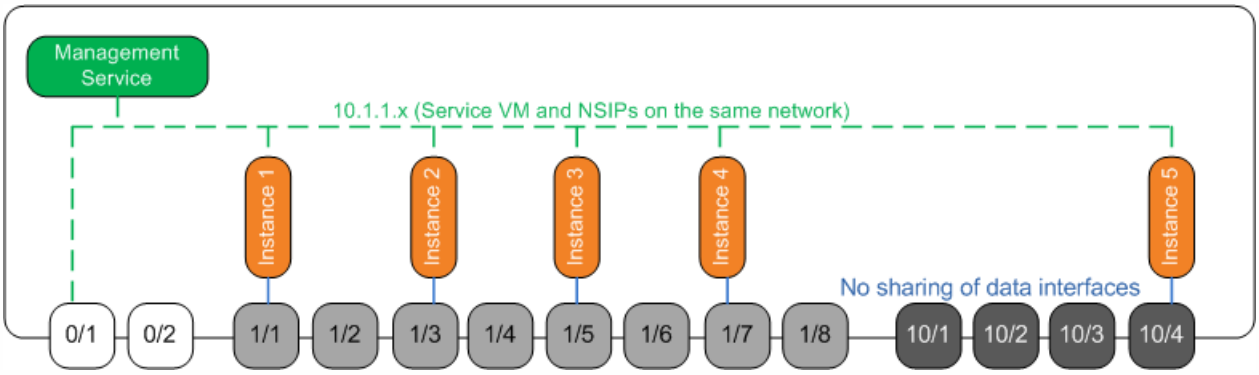
May 04, 2017

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

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

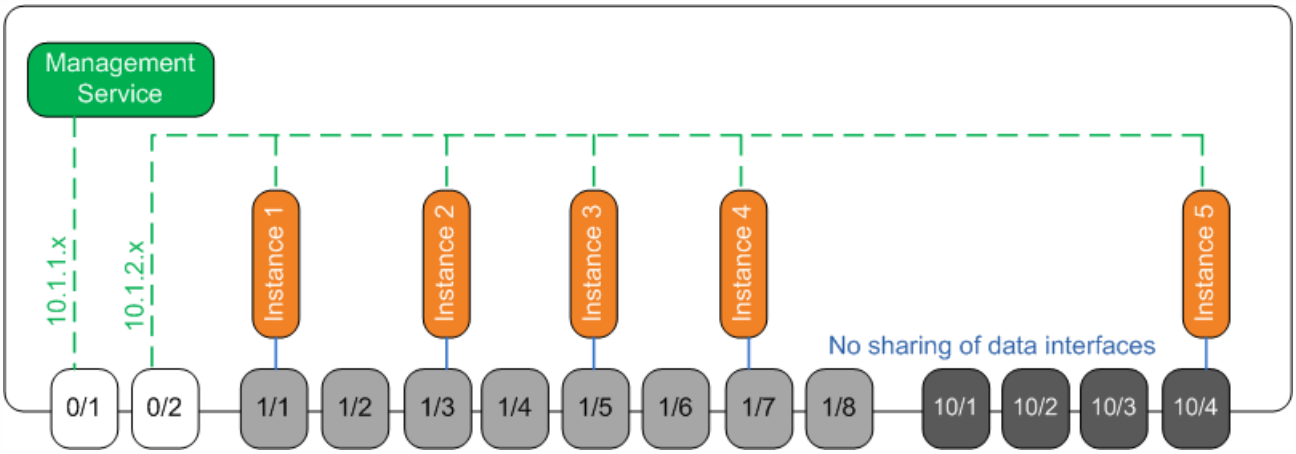
May 04, 2017

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

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

May 04, 2017

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.

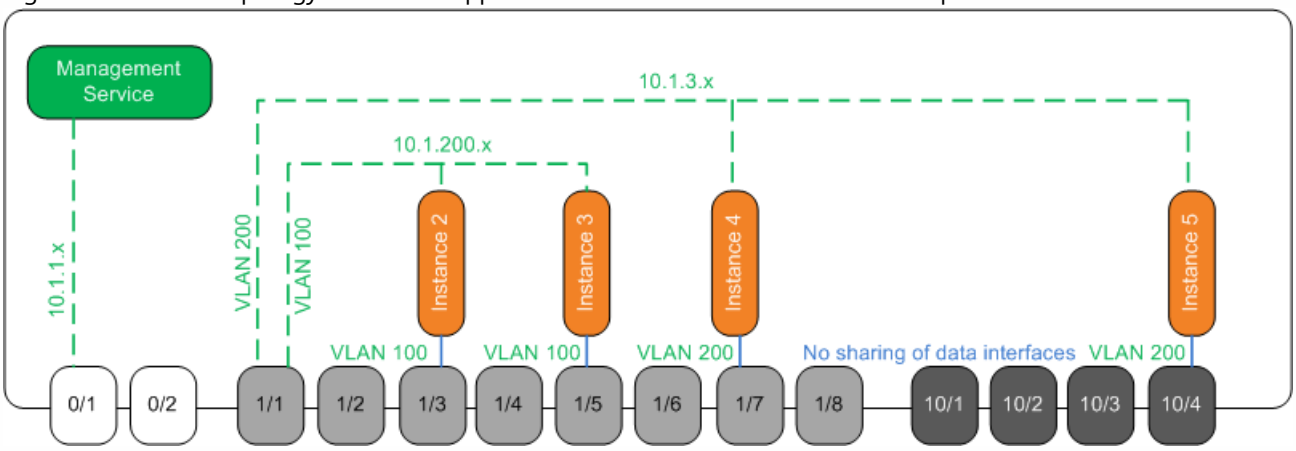
Consolidation with Dedicated Interfaces for Each Instance

May 04, 2017

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

The following figure illustrates the above use case.

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



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

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

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

Parameter Name Admin Profile	Values for Instance 5 ns_nsroot_profile	Values for Instance 3 ns_nsroot_profile
User Name	vpx5	vpx3
Password	Sdx	root
Confirm Password	Sdx	root
Shell/Sftp/Scp Access	True	True
Total Memory (MB)	2048	2048
#SSL Chips	1	1
Throughput (Mbps)	1000	1000
Packets per second	1000000	1000000
CPU	Shared	Shared
Interface	1/1 and 10/4	1/1 and 1/5
NSVLAN	200	100
Add (interface)	1/1	1/1
Tagged Interface	Select Tagged	Select Tagged

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

May 04, 2017

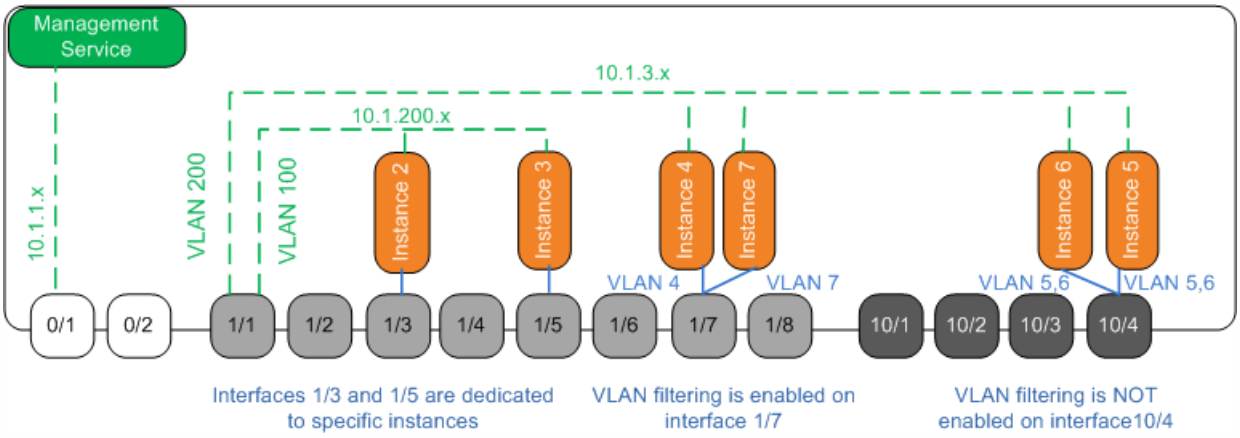
You can enable and disable VLAN filtering on an interface as required. For example, if you need to configure more than 100 VLANs on an instance, assign a dedicated physical interface to that instance and disable VLAN filtering on that interface. Enable VLAN filtering on instances that share a physical 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	vpx7	vpx4
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	vpx4	vpx4
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

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.

Third-Party Virtual Machines

May 04, 2017

The NetScaler SDX appliance supports provisioning of the following third-party virtual machines (instances):

- SECUREMATRIX GSB
- InterScan Web Security
- 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.

When you configure third-party virtual machines, then 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 third-party virtual machines.

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

May 04, 2017

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.

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.

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 SECUREMATRX 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

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.

InterScan Web Security

May 04, 2017

InterScan Web Security is a software virtual appliance which dynamically protects against traditional and emerging web threats at the Internet gateway. By integrating application control, anti-malware scanning, real-time web reputation, flexible URL filtering, and advanced threat protection it delivers superior protection and greater visibility and control over the growing use of cloud-based applications on the network. Real-time reporting and centralized management give your administrators a proactive decision making tool, enabling on the spot risk management.

InterScan Web Security:

- Allows deeper visibility into end-user Internet activity
- Centralizes management for maximum control
- Monitors web use as it happens
- Enables on-the-spot remediation
- Reduces appliance sprawl and energy costs
- Provides optional data loss protection and sandbox executional analysis

Before you can provision an InterScan Web Security instance, you must download an XVA image from the Trend Micro website. After you have downloaded the XVA image, upload it to the NetScaler SDX appliance.

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 InterScan Web Security instance.

To upload an XVA image to the SDX appliance:

1. From the Configuration tab, navigate to TrendMicro IWSVA > Software Images.
2. In the details pane, under XVA Files tab , 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 TrendMicro IWSVA instance

1. On the Configuration tab, navigate to TrendMicro IWSVA > Instances.
2. In the details pane, click Add.
3. In the Provision TrendMicro IWSVA wizard, follow the instructions on the screen.
4. Click OK, 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 Edit. In the Modify TrendMicro IWSVA wizard, set the parameters to values suitable for your environment.

Websense Protector

May 04, 2017

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 setup 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

May 04, 2017

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/.

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.

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 BlueCat DNS/DHCP instance.

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.

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.

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.

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.

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

May 04, 2017

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: 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 CA Access Gateway instance. 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.

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. 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 Pingmessage 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

May 04, 2017

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 or Python, 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.
- 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.
- For Python clients, you must have a system where Python 2.7 or above version and the Requests library (available in <NITRO_SDK_HOME>/lib) is installed.

Obtaining the NITRO Package

May 04, 2017

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:

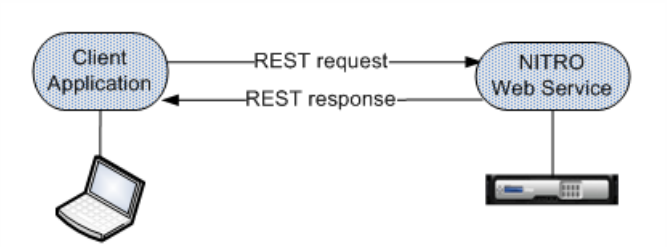
- The REST package contains only documentation for using the REST interfaces.
- For the Python SDK, the library must be installed on the client path. For installation instructions, read the <NITRO_SDK_HOME>/README.txt file.

How NITRO Works

May 04, 2017

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

May 04, 2017

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

System APIs

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

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

Note: You must have a user account on that appliance. The configuration operations that you can perform are limited by the administrative role assigned to your account.
The following sample code connects to a NetScaler SDX appliance with IP address 10.102.31.16 by using HTTPS protocol:

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

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

Note: You must use the nitro_service object in all further NITRO operations on the appliance.
To disconnect from the appliance, invoke the logout() method as follows:

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

Configuration APIs

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

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

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

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

Creating a Resource

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

1. Set the value for the required properties of the resource by using the corresponding property name. The result is a resource object that contains the details required for the resource.
   Note: These values are set locally on the client. The values are not reflected on the appliance till the object is uploaded.
2. Upload the resource object to the appliance, using the static add() method.

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

```
ns newns = new ns();

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

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

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

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

newns.set_network_interfaces(interface_array);

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

Retrieving Resource Details

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

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

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

```
//Retrieve the resource object from the NetScaler SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
System.out.println(returned_ns[i].get_ip_address());
System.out.println(returned_ns[i].get_netmask());
```

Retrieving Resource Statistics

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

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

```
ns obj = new ns();
obj.set_id("123456a");
ns stats = ns.get(nitroservice, obj);
System.out.println("CPU Usage:" + stats.get_ns_cpu_usage());
System.out.println("Memory Usage:" + stats.get_ns_memory_usage());
System.out.println("Request rate/sec:" +stats.get_http_req());
```

Updating a Resource

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

1. Set the id property to the ID of the resource to be updated.
2. Set the value for the required properties of the resource by using the corresponding property name. The result is a resource object.
   Note: These values are set locally on the client. The values are not reflected on the appliance till the object is uploaded.
3. Upload the resource object to the appliance, using the update() method.

The following sample code updates the name of the NetScaler instance with ID 123456a to 'ns_instance_new':

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.set_id("123456a");

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally
update_obj.set_name("ns_instance_new");

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
```

Deleting a Resource

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

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

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

Bulk Operations

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

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

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

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

Note: You must configure the required behavior while establishing a connection with the appliance, by setting the onerror param in the nitro_service() method.
The following sample code adds two NetScalers in one operation:

```
ns[] newns = new ns[2];

//Specify details of first NetScaler
newns[0] = new ns();
newns[0].set_name("ns_instance1");
newns[0].set_ip_address("10.70.136.5");
newns[0].set_netmask("255.255.255.0");
newns[0].set_gateway("10.70.136.1");
...
...
...

//Specify details of second NetScaler
newns[1] = new ns();
newns[1].set_name("ns_instance2");
newns[1].set_ip_address("10.70.136.8");
newns[1].set_netmask("255.255.255.0");
newns[1].set_gateway("10.70.136.1");
...
...

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

Exception Handling

The errorcode field indicates the status of the operation.

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

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

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

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

.NET SDK

May 04, 2017

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

System APIs

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

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

Note: You must have a user account on that appliance. The configuration operations that you can perform are limited by the administrative role assigned to your account.
The following sample code connects to a NetScaler SDX appliance with IP address 10.102.31.16 by using HTTPS protocol:

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

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

Note: You must use the nitro_service object in all further NITRO operations on the appliance.
To disconnect from the appliance, invoke the logout() method as follows:

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

Configuration APIs

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

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

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

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

Creating a Resource

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

1. Set the value for the required properties of the resource by using the corresponding property name. The result is a resource object that contains the details required for the resource.
   Note: These values are set locally on the client. The values are not reflected on the appliance till the object is uploaded.
2. Upload the resource object to the appliance, using the static add() method.

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

```
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.name = "ns_instance";
newns.ip_address = "10.70.136.5";
newns.netmask = "255.255.255.0";
newns.gateway = "10.70.136.1";
newns.image_name = "nsvpx-9.3.45_nc.xva";
newns.profile_name = "ns_nsroot_profile";
newns.vm_memory_total = 2048;
newns.throughput = 1000;
newns.pps = 1000000;
newns.license = "Standard";
newns.username = "admin";
newns.password = "admin";

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

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

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

newns.network_interfaces = interface_array;

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

Retrieve Resource Details

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

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

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

```
//Retrieve the resource object from the NetScaler SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
Console.WriteLine(returned_ns[i].ip_address);
Console.WriteLine(returned_ns[i].netmask);
```

Retrieve Resource Statistics

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

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

```
ns obj = new ns();
obj.id = "123456a";
ns stats = ns.get(nitroservice, obj);
Console.WriteLine("CPU Usage:" + stats.ns_cpu_usage);
Console.WriteLine("Memory Usage:" + stats.ns_memory_usage);
Console.WriteLine("Request rate/sec:" +stats.http_req);
```

Updating a Resource

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

1. Set the id property to the ID of the resource to be updated.
2. Set the value for the required properties of the resource by using the corresponding property name. The result is a resource object.
   Note: These values are set locally on the client. The values are not reflected on the appliance till the object is uploaded.
3. Upload the resource object to the appliance, using the update() method.

The following sample code updates the name of the NetScaler instance with ID 123456a to 'ns_instance_new':

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.id = "123456a";

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally
update_obj.name = "ns_instance_new";

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
```

Deleting a Resource

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

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

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

Bulk Operations

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

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

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

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

Note: You must configure the required behavior while establishing a connection with the appliance, by setting the onerror param in the nitro_service() method.
The following sample code adds two NetScalers in one operation:

```
ns[] newns = new ns[2];

//Specify details of first NetScaler
newns[0] = new ns();
newns[0].name = "ns_instance1";
newns[0].ip_address = "10.70.136.5";
newns[0].netmask = "255.255.255.0";
newns[0].gateway = "10.70.136.1";
...
...

//Specify details of second NetScaler
newns[1] = new ns();
newns[1].name = "ns_instance2";
newns[1].ip_address = "10.70.136.8";
newns[1].netmask = "255.255.255.0";
newns[1].gateway = "10.70.136.1";
...
...

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

Exception Handling

The errorcode field indicates the status of the operation.

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

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

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

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

REST Web Services

May 04, 2017

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

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

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

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

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

System APIs

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/v2/config/login/
- **HTTP Method.** POST
- **Request.**
  - **Header**
    Content-Type:application/vnd.com.citrix.sdx.login+json
    Note: Content types such as 'application/x-www-form-urlencoded' that were supported in earlier versions of NITRO can also be used. You must make sure that the payload is the same as used in earlier versions. The payloads provided in

this documentation are only applicable if the content type is of the form 'application/vnd.com.citrix.sdx.login+json'.

- **Payload**

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

- **Response Payload.**
  - **Header**

    HTTP/1.0 201 Created
    Set-Cookie:
    NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2

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:

```
{
   "login":
   {
      "username":"nsroot",
      "password":"verysecret",
      "timeout":3600
   }
}
```

You can also connect to the appliance to perform a single operation, by specifying the username and password in the request header of the operation. For example, to connect to an appliance while creating a NetScaler instance:

- **URL.** https://10.102.31.16/nitro/v2/config/ns/
- **HTTP Method.** POST
- **Request.**
  - **Header**

    X-NITRO-USER:nsroot
    X-NITRO-PASS:verysecret
    Content-Type:application/vnd.com.citrix.sdx.ns+json
  - **Payload**

```
{
   "ns":
   {
      ...
   }
}
```

- **Response.**
  - **Header**

    HTTP/1.0 201 Created

To disconnect from the appliance, use the DELETE method:

- **URL.** https://10.102.31.16/nitro/v2/config/login/
- **HTTP Method.** DELETE
- **Request.**
  - **Header**
    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.sdx.login+json

Configuration APIs

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/v2/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/v2/config/ns/
- **HTTP Method.** POST
- **Request.**
  - **Header**
    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.sdx.ns+json
  - **Payload**

```
{
   "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/v2/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/v2/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/v2/config/<resource_type>?count=yes.

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

- **URL.** http://10.102.31.16/nitro/v2/config/ns/123456a
- **HTTP Method.** GET

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/v2/config/ns/
- **HTTP Method.** PUT
- **Request Payload.**
  - **Header**
    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.sdx.ns+json
  - **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/v2/config/ns/123456a
- **HTTP Method.** DELETE
- **Request.**
  - **Header**
    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.sdx.ns+json

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/v2/config/ns/
- **HTTP Method.** POST
- **Request Payload.**
  - **Header**
    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.sdx.ns+json
    X-NITRO-ONERROR:continue
  - **Payload**

```
{
   "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/v2/config/ns/
- **HTTP Method.** POST
- **Request Payload.**
  - **Header**
    Cookie:NITRO_AUTH_TOKEN=tokenvalue
    Content-Type:application/vnd.com.citrix.sdx.ns+json
    X-NITRO-ONERROR:continue
  - **Payload**

```
{
  "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"
    }
  ],
   "mpsuser":
  [
    {
      "name":"admin",
      "password":"admin",
      "permission":"superuser"
    },
    {
      "name":"admin",
      "password":"admin",
      "permission":"superuser"
    }
```



```
        ]
    }
```

Exception Handling

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.

Converting a NetScaler MPX Appliance to a NetScaler SDX Appliance

Nov 03, 2016

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 8005/8010/8015/8200/8400/8600/8800 appliances to NetScaler SDX 8010/8015/8400/8600 appliances by upgrading the software through a new Solid State Drive (SSD).

The Citrix NetScaler models SDX 8010/8015/8400/8600 are 1U appliances. Each model has one quad-core processor (8 cores with hyper-threading) and 32 gigabytes (GB) of memory. The SDX 8010/8015/8400/8600 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+)

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

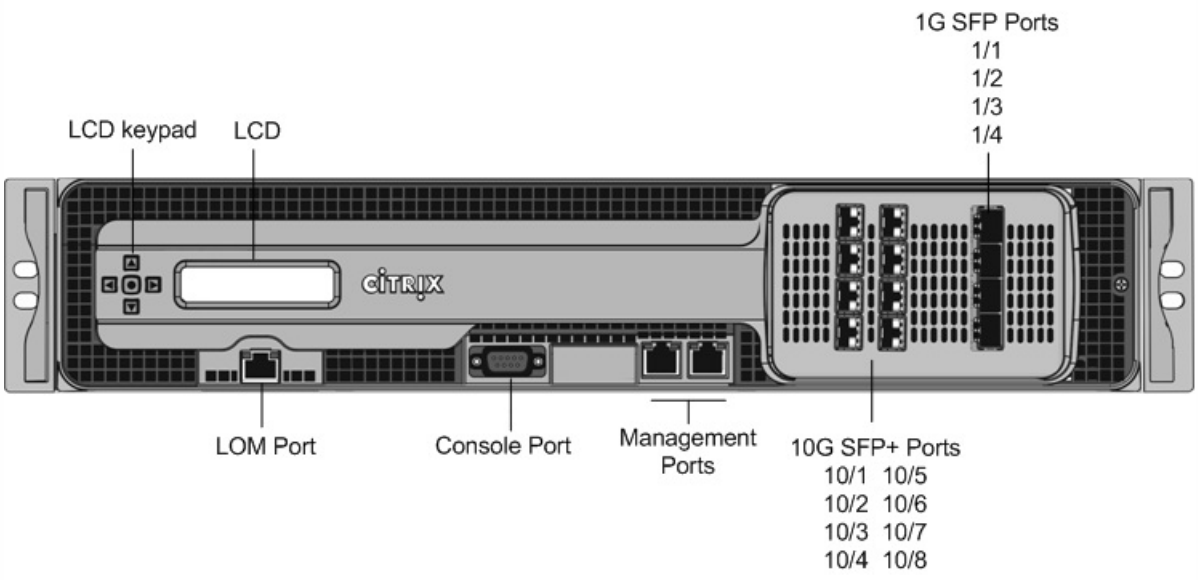
Connect one end of the console cable to the RS232 serial port on the appliance, and the other end to the computer or terminal.

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
```

7. 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.
8. At the NetScaler command line interface, switch to the shell prompt. Type: **shell**
9. 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 0xddd00000-0xddddfffff irq 24 at device 0.0 on pci20
   Cavium cavium_probe : found card  0x177d,device=0x11
   cavium1 mem 0xd6f00000-0xd6ffffff 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_ioctl (cpu 7, NSPPE-03): Reserving 596 MB for shared memory type 0
   ```
10. 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 newnslog files to be processed...
Generating the events from newnslog 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#
```

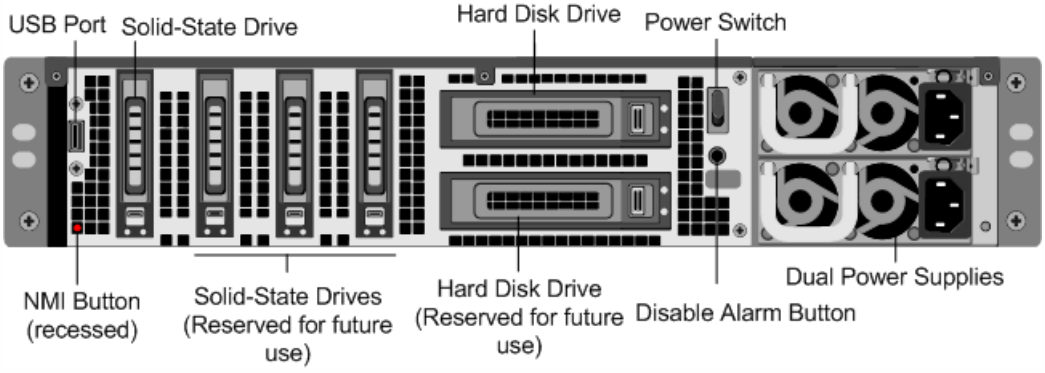
13. **Important**: Physically disconnect all ports except the LOM port, including the management port, from the network.
14. At the shell prompt, switch to the NetScaler command line. Type: **exit**
15. Run the following command to shut down the appliance: **shutdown -p now**

    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.

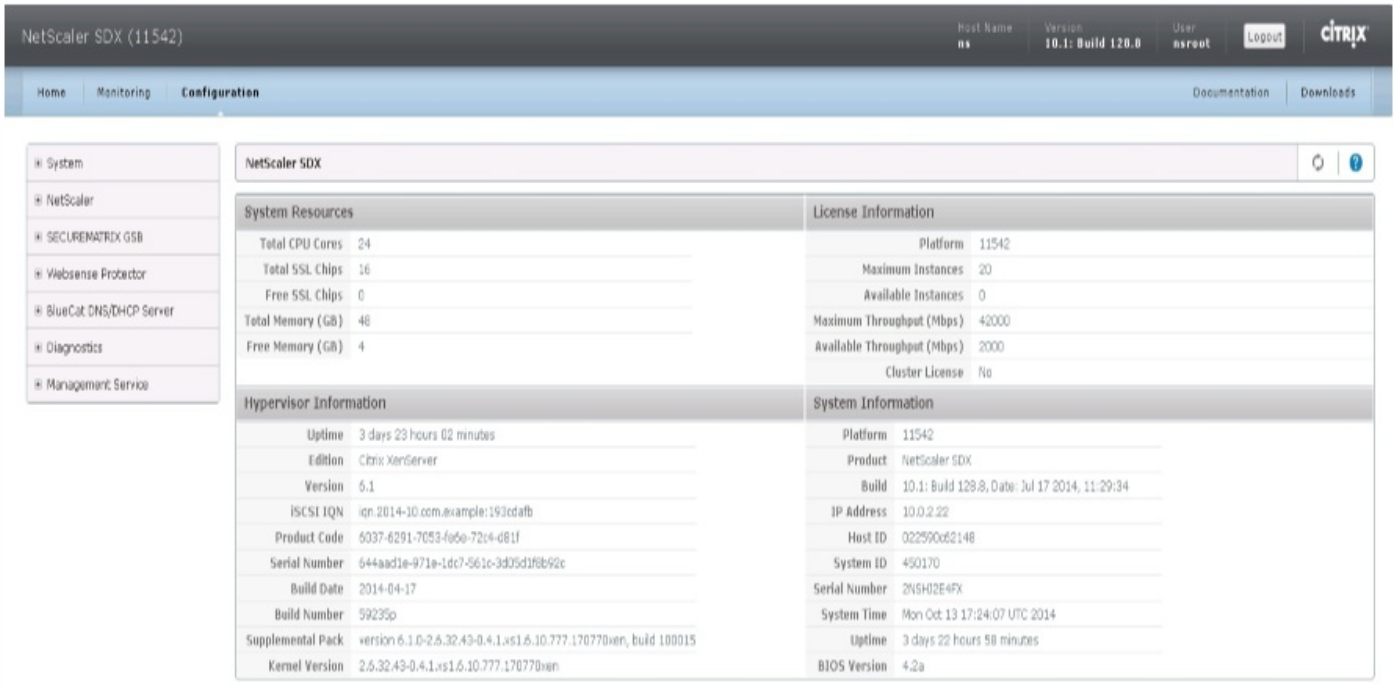
Note: The serial number of the appliance remains the same.

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.



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 8005/8010/8015/8200/8400/8600/8800 Appliance to a NetScaler SDX 8010/8015/8400/8600 Appliance

Nov 03, 2016

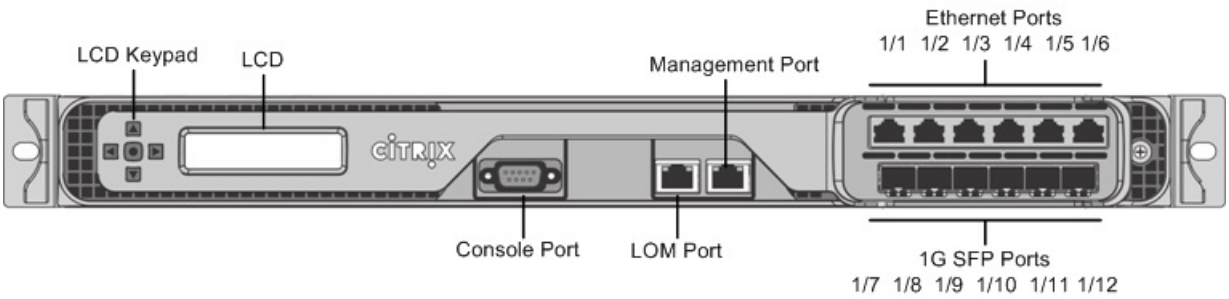
To convert a NetScaler 8005/8010/8015/8200/8400/8600/8800 appliance to a NetScaler SDX 8010/8015/8400/8800 appliance, you must access the appliance through a console cable attached to a computer or terminal.

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 8005/8010/8015/8200/8400/8600/8800 appliance to a NetScaler SDX 8010/8015/8400/8600 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

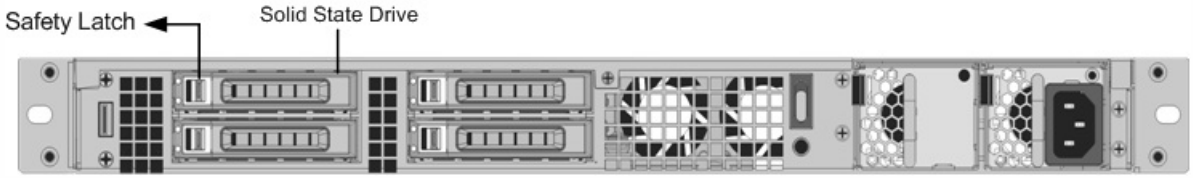
> enable interface 10/x

where x is the new interface number.

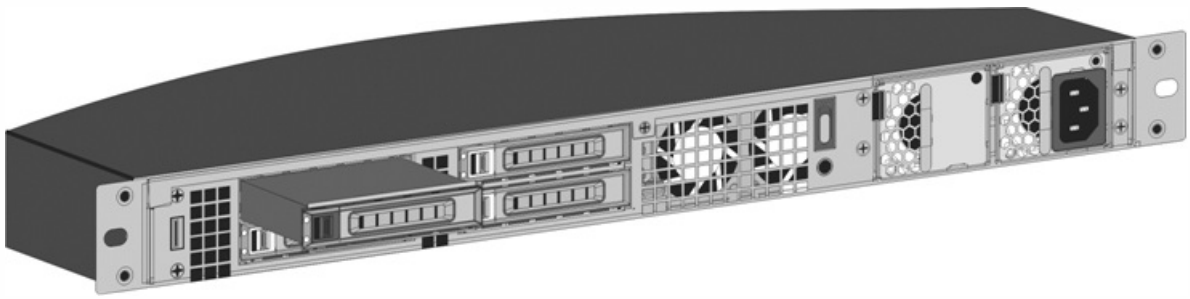
8. For any interface that you do not want to use after conversion, run the following commands:
   > disable interface 1/x

   > 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 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).

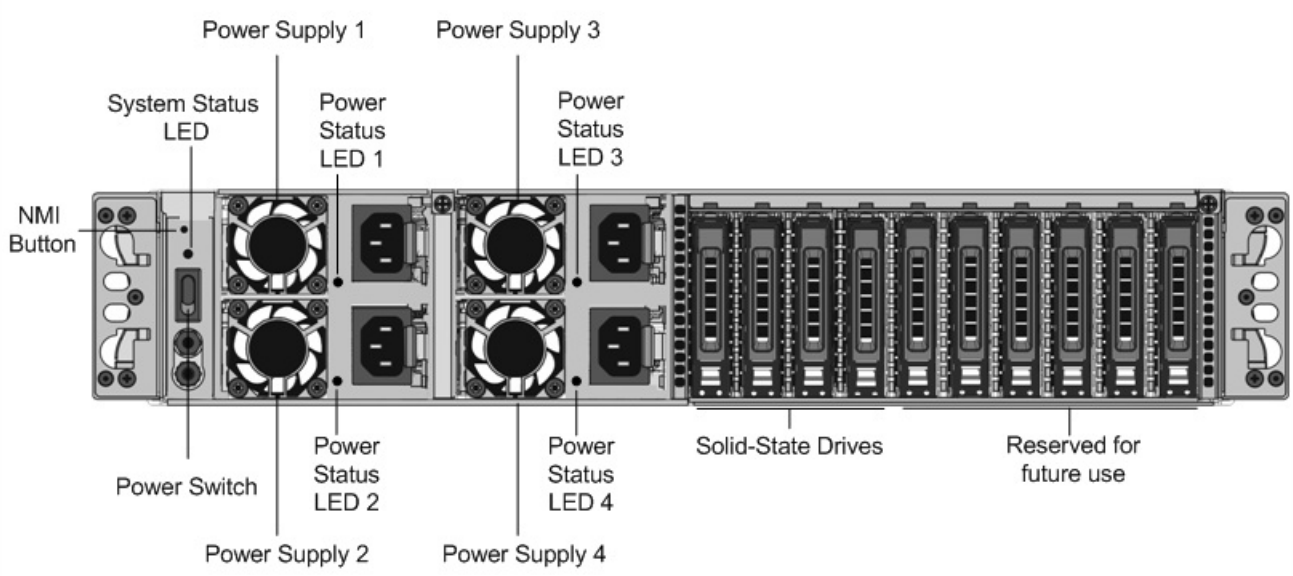
After the conversion process, you make a few modifications to the appliance's configuration and apply a new license. You can then provision the VPX instances through the Management Service on what is now a NetScaler SDX appliance.

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.

SDX Command Reference

Aug 18, 2015

A detailed list of the commands that can be used to configure the SDX appliance through the CLI.

System

Aug 18, 2015

The entities on which you can perform NetScaler SDX CLI operations:

- aaaserver - AAA Server configuration
- admindomainInfo - Administrative Domain Information
- backup - backup
- backupfile - Backup files
- backuppolicy - Backup Policy
- deviceprofile - Device Profile
- hostname - System Hostname
- ip_block - This collection holds private ip block information.
- ldapserver - LDAP Server
- license - License Information
- licensefile - License File
- mailprofile - Mail profile
- manageddevice - Managed Device
- managementservicestatistics - Health Monitoring Stats
- networkconfig - SDX Network Configuration
- networkpool - Network Pool
- ntpparam - NTP Parameters
- ntpserver - NTP Server
- ntpsync - NTP Sync
- passwordpolicy - Password Policy configuration
- prunepolicy - Prune Policy
- radiusserver - Radius Server configuration
- rediscover - Inventory
- singlebundleimage - CBSDX Single Bundle Build File
- singlebundleinfo - Single Bundle File Info
- singlebundleupgrade - CBSDX Single Bundle Upgrade
- smsprofile - SMS profile
- smsserver - SMS server properties
- smtpserver - SMTP server properties
- snmpalarm - SNMP Alarm Configurations
- snmpinfo - SNMP Information
- snmpmanager - SNMP Agent Manager configuration
- snmpmib - SNMP MIB Information
- snmptrap - SNMP Trap Destinations
- snmpuser - SNMP User
- snmpview - SNMP view
- sslcertfile - SSL certificate File
- sslcertificate - Install SSL certificate on Management Service
- sslkeyfile - SSL key File
- sslsettings - SSL Settings
- sslv3Setting - SSLV3 Setting

- syslogparameters - Syslog Parameters
- syslogserver - Syslog Server
- systembackuprestore - Backup
- systemgroup - System Groups
- systemimage - System Build File
- systemsession - Client Session
- systemsettings - System Settings
- systemstatus - System Status
- systemupgrade - System Upgrade
- systemuser - System User
- tacacsserver - TACACS Server configuration
- techsupport - Technical Support
- tenant - Tenant on SDX Platform
- timezone - Current timezone
- userlockoutpolicy - User Lockout Policy configuration
- vlandetails - VLAN details
- vlansummary - VLAN summary
- vmdevice - VM Device

aaaserver

Aug 18, 2015

AAA Server configuration

show | set

show aaaserver

Use this operation to get AAA server details

Synopsys

show aaaserver [id=<string>]

Parameters

id

Id is system generated key for all the radius servers

---

set aaaserver

Use this operation to modify AAA server details

Synopsys

set aaaserver primary_server_type=<string> [fallback_local_authentication=(false | true)] [primary_server_name=<string>]

Parameters

primary_server_type

Type of primary server. Support Types 1. LOCAL 2.RADIUS 3.LDAP 4.TACACS 5.KEYSTONE

This is a mandatory parameter.

fallback_local_authentication

Enable local fallback authentication

primary_server_name

Name of primary server name

---

admindomainInfo

Aug 18, 2015

Administrative Domain Information

show admindomainInfo

Use this operation to get administrative domain info

Synopsys

show admindomainInfo

backup

Aug 18, 2015

backup

show | add

show backup

Use this operation to get backup component information

Synopsys

show backup

---

add backup

Use this operation to Backup the Appliance

Synopsys

add backup [backup_file_name=<string>]

Parameters

backup_file_name

Backup file name

---

backupfile

Aug 18, 2015

Backup files

show | delete

show backupfile

Use this operation to get backup file

Synopsys

show backupfile [file_name=<string>]

Parameters

file_name

File Name

---

delete backupfile

Use this operation to delete backup file

Synopsys

delete backupfile file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

backuppolicy

Aug 18, 2015

Backup Policy

show | set

show backuppolicy

Use this operation to get backup policy to view the number of previous backups to retain

Synopsys

show backuppolicy [policy_name=<string>]

Parameters

policy_name

Policy Name

---

set backuppolicy

Use this operation to modify the number of previous backups to retain

Synopsys

set backuppolicy backup_to_retain=<int> [policy_name=<string>]

Parameters

backup_to_retain

Number of previous backups to retain

This is a mandatory parameter.

policy_name

Policy Name

---

deviceprofile

Aug 18, 2015

Device Profile

show deviceprofile

Use this operation to get device profiles

Synopsys

show deviceprofile [id=<string>]

Parameters

id

Id is system generated key for all the device profiles

hostname

Aug 18, 2015

System Hostname

show | set

show hostname

Use this operation to get the hostname

Synopsys

show hostname

---

set hostname

Use this operation to modify hostname

Synopsys

set hostname [hostname=<string>]

Parameters

hostname

Hostname

---

ip_block

Aug 18, 2015

This collection holds private ip block information.

show | delete | set | add

show ip_block

Use this operation to get ip block

Synopsys

show ip_block [id=<string>]

Parameters

id

Id is IP block name

---

delete ip_block

Use this operation to delete ip block(s)

Synopsys

delete ip_block id=<string>

Parameters

id

Id is IP block name

This is a mandatory parameter.

---

set ip_block

Use this operation to modify ip block

Synopsys

set ip_block id=<string> [end_ip_num=<doublelong>] [region_code=<string>] [description=<string>] [start_ip_num=<doublelong>] [name=<string>] [longitude=<double>] [latitude=<double>] [country_code=<string>] [city=<string>] [region=<string>] [start_ip=<ipaddress>] [end_ip=<ipaddress>] [country=<string>]

Parameters

id

Id is IP block name

This is a mandatory parameter.

end_ip_num

end_ip_num

region_code

region_code

description

Description about Ip Block

start_ip_num

start_ip_num

name

name

longitude

longitude

latitude

latitude

country_code

country_code

city

city

region

region

start_ip

start_ip

end_ip

end_ip

country

country

add ip_block

Use this operation to add ip block

Synopsys

add ip_block [end_ip_num=<doublelong>] [region_code=<string>] [description=<string>] [start_ip_num=<doublelong>] [name=<string>] [longitude=<double>] [latitude=<double>] [country_code=<string>] [city=<string>] [region=<string>] [start_ip=<ipaddress>] [end_ip=<ipaddress>] [country=<string>]

Parameters

end_ip_num

end_ip_num

region_code

region_code

description

Description about Ip Block

start_ip_num

start_ip_num

name

name

longitude

longitude

latitude

latitude

country_code

country_code

city

city

region

region

start_ip

start_ip

end_ip

end_ip

country

country

ldapserver

Aug 18, 2015

LDAP Server

show | delete | set | add

show ldapserver

Use this operation to get LDAP server details

Synopsys

show ldapserver [id=<string>]

Parameters

id

Id is system generated key for all the ldap servers

---

delete ldapserver

Use this operation to delete LDAP server

Synopsys

delete ldapserver id=<string>

Parameters

id

Id is system generated key for all the ldap servers

This is a mandatory parameter.

---

set ldapserver

Use this operation to modify LDAP server

Synopsys

set ldapserver id=<string> name=<string> ip_address=<ipaddress> [port=<int>] [validate_ldap_server_certs=(false | true)] [ldap_host_name=<string>] [sec_type=<string>] [type=<string>] [subattribute_name=<string>] [change_password=(false | true)] [follow_referrals=(false | true)] [max_nesting_level=<int>] [group_search_filter=<string>] [group_attr_name=<string>] [max_ldap_referrals=<int>] [group_search_attribute=<string>] [group_search_subattribute=<string>] [auth_timeout=<int>] [nested_group_extraction=(false | true)] [group_name_identifier=<string>] [default_authentication_group=<string>] [bind_passwd=<stringx>] [bind_dn=<string>] [search_filter=<string>]

[login_name=<string>] [base_dn=<string>]

Parameters

id

Id is system generated key for all the ldap servers

This is a mandatory parameter.

name

Name of LDAP server

This is a mandatory parameter.

ip_address

The IP address of the LDAP server.

This is a mandatory parameter.

port

The port number on which the LDAP server is running

validate_ldap_server_certs

Validate LDAP Server Certificate

ldap_host_name

Host Name on the certificate from LDAP Server

sec_type

The communication type between the system and the LDAP server

type

The type of LDAP server

subattribute_name

The Sub-Attribute name for group extraction from LDAP server

change_password

Enable change of the user

follow_referrals

Enable following LDAP referrals received from LDAP server

max_nesting_level

Number of levels at which group extraction is allowed

group_search_filter

String to be combined with the default LDAP group search string to form the search value

group_attr_name

The Attribute name for group extraction from the LDAP server

max_ldap_referrals

Maximum number of ldap referrals to follow

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.

auth_timeout

The maximum number of seconds the system will wait for a response from the LDAP server

nested_group_extraction

Enable Nested Group Extraction

group_name_identifier

Name that uniquely identifies a group in LDAP server

default_authentication_group

This is the default group

bind_passwd

The password used to bind to the LDAP server

bind_dn

The full distinguished name used to bind to the LDAP server

search_filter

The String to be combined with the default LDAP user search string to form the value

login_name

The name attribute used by the system to query the external LDAP server

base_dn

The base or node where the ldapsearch should start

---

add ldapserver

Use this operation to add LDAP server

Synopsys

add ldapserver type=<string> name=<string> ip_address=<ipaddress> [port=<int>] [validate_ldap_server_certs=(false | true)] [ldap_host_name=<string>] [sec_type=<string>] [subattribute_name=<string>] [change_password=(false | true)] [follow_referrals=(false | true)] [max_nesting_level=<int>] [group_search_filter=<string>] [group_attr_name=<string>] [max_ldap_referrals=<int>] [group_search_attribute=<string>] [group_search_subattribute=<string>] [auth_timeout=<int>] [nested_group_extraction=(false | true)] [group_name_identifier=<string>] [default_authentication_group=<string>] [bind_passwd=<stringx>] [bind_dn=<string>] [search_filter=<string>] [login_name=<string>] [base_dn=<string>]

Parameters

type

The type of LDAP server

This is a mandatory parameter.

name

Name of LDAP server

This is a mandatory parameter.

ip_address

The IP address of the LDAP server.

This is a mandatory parameter.

port

The port number on which the LDAP server is running

validate_ldap_server_certs

Validate LDAP Server Certificate

ldap_host_name

Host Name on the certificate from LDAP Server

sec_type

The communication type between the system and the LDAP server

subattribute_name

The Sub-Attribute name for group extraction from LDAP server

change_password

Enable change of the user

follow_referrals

Enable following LDAP referrals received from LDAP server

max_nesting_level

Number of levels at which group extraction is allowed

group_search_filter

String to be combined with the default LDAP group search string to form the search value

group_attr_name

The Attribute name for group extraction from the LDAP server

max_ldap_referrals

Maximum number of ldap referrals to follow

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.

auth_timeout

The maximum number of seconds the system will wait for a response from the LDAP server

nested_group_extraction

Enable Nested Group Extraction

group_name_identifier

Name that uniquely identifies a group in LDAP server

default_authentication_group

This is the default group

bind_passwd

The password used to bind to the LDAP server

bind_dn

The full distinguished name used to bind to the LDAP server

search_filter

The String to be combined with the default LDAP user search string to form the value

login_name

The name attribute used by the system to query the external LDAP server

base_dn

The base or node where the ldapsearch should start

license

Aug 18, 2015

License Information

show | do custom

show license

Use this operation to get SDX license information

Synopsys

show license

---

do license custom

Use this operation to apply new licenses files

Synopsys

do license custom

---

licensefile

Aug 18, 2015

License File

show | delete

show licensefile

Use this operation to get license file

Synopsys

show licensefile [file_name=<string>]

Parameters

file_name

File Name

---

delete licensefile

Use this operation to delete license file

Synopsys

delete licensefile file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

mailprofile

Aug 18, 2015

Mail profile

show | delete | set | add

show mailprofile

Use this operation to get mail profile.

Synopsys

show mailprofile [id=<string>]

Parameters

id

Id is system generated key for all the mail profile.

---

delete mailprofile

Use this operation to delete mail profile.

Synopsys

delete mailprofile id=<string>

Parameters

id

Id is system generated key for all the mail profile.

This is a mandatory parameter.

---

set mailprofile

Use this operation to modify mail profile.

Synopsys

set mailprofile id=<string> [to_list=<string>] [server_name=<internethost>] [cc_list=<string>] [profile_name=<string>] [bcc_list=<string>] [sender_mail_address=<string>]

Parameters

id

Id is system generated key for all the mail profile.

This is a mandatory parameter.

to_list

List of to whom send the mail.

server_name

SMTP server name

cc_list

List to whom CC the mail.

profile_name

Profile name for the mail setting.

bcc_list

List to whom BCC the mail.

sender_mail_address

Email Address from where mail is send

---

add mailprofile

Use this operation to add mail profile.

Synopsys

add mailprofile to_list=<string> server_name=<internethost> profile_name=<string> [cc_list=<string>] [bcc_list=<string>] [sender_mail_address=<string>]

Parameters

to_list

List of to whom send the mail.

This is a mandatory parameter.

server_name

SMTP server name

This is a mandatory parameter.

profile_name

Profile name for the mail setting.

This is a mandatory parameter.

cc_list

List to whom CC the mail.

bcc_list

List to whom BCC the mail.

sender_mail_address

Email Address from where mail is send

manageddevice

Aug 18, 2015

Managed Device

show manageddevice

Use this operation to get managed devices

Synopsys

show manageddevice [id=<string>]

Parameters

id

Id is system generated key for all the managed devices

managementservicestatistics

Aug 18, 2015

Health Monitoring Stats

show managementservicestatistics

Use this operation to get health stats

Synopsys

show managementservicestatistics [id=<string>]

Parameters

id

Id is system generated key

networkconfig

Aug 18, 2015

SDX Network Configuration

show | set

show networkconfig

Use this operation to get SDX network configuration

Synopsys

show networkconfig

---

set networkconfig

Use this operation to modify SDX network configuration

Synopsys

set networkconfig gateway=<ipaddress> xen_ip_address=<ipaddress> network_interface=<string> svm_ip_address=<ipaddress> netmask=<ipaddress> [dns=<ipaddress>] [init_status=<int>] [act_id=<string>]

Parameters

gateway

Gateway

This is a mandatory parameter.

xen_ip_address

XenServer IP Address

This is a mandatory parameter.

network_interface

Interface on which management needs to be enabled

This is a mandatory parameter.

svm_ip_address

Management Service IP Address

This is a mandatory parameter.

netmask

Netmask

This is a mandatory parameter.

dns

DNS Server

init_status

System initialize status

act_id

Activity Id

---

networkpool

Aug 18, 2015

Network Pool

show networkpool

Use this operation to get the network pool

Synopsys

show networkpool [id=<string>]

Parameters

id

Id is system generated key for all the networks

ntpparam

Aug 18, 2015

NTP Parameters

show | set

show ntpparam

Use this operation to get NTP Server

Synopsys

show ntpparam

---

set ntpparam

Use this operation to modify NTP Server

Synopsys

set ntpparam [trusted_key_list=<int...>] [automax_logsec=<int>] [authentication=(false | true)] [revoke_logsec=<int>]

Parameters

trusted_key_list

List of Trusted Key Identifiers for Symmetric Key Cryptography

automax_logsec

Automax Interval (as power of 2 in seconds)

authentication

Authentication Enabled

revoke_logsec

Revoke Interval (as power of 2 in seconds)

---

ntpserver

Aug 18, 2015

NTP Server

show | delete | set | add

show ntpserver

Use this operation to get NTP Server

Synopsys

show ntpserver [server=<internethost>]

Parameters

server

NTP Time Server Address

---

delete ntpserver

Use this operation to delete NTP Server

Synopsys

delete ntpserver [server=<internethost>]

Parameters

server

NTP Time Server Address

---

set ntpserver

Use this operation to modify NTP Server

Synopsys

set ntpserver [minpoll=<int>] [preferred_server=(false | true)] [server=<internethost>] [autokey=(false | true)] [key_id=<int>] [maxpoll=<int>] [client=<string>]

Parameters

minpoll

Minimum Poll Interval

preferred_server

NTP Server Preferred

server

NTP Time Server Address

autokey

Autokey Public Key Authentication

key_id

Key Identifier for Symmetric Key Authentication

maxpoll

Maximum Poll Interval

client

Sender of request, whether from Setup Wizard or direct NTP configuration

---

add ntpserver

Use this operation to add NTP Server

Synopsys

add ntpserver server=<internethost> [minpoll=<int>] [preferred_server=(false | true)] [autokey=(false | true)] [key_id=<int>] [maxpoll=<int>] [client=<string>]

Parameters

server

NTP Time Server Address

This is a mandatory parameter.

minpoll

Minimum Poll Interval

preferred_server

NTP Server Preferred

autokey

Autokey Public Key Authentication

key_id

Key Identifier for Symmetric Key Authentication

maxpoll

Maximum Poll Interval

client

Sender of request, whether from Setup Wizard or direct NTP configuration

---

ntpsync

Aug 18, 2015

NTP Sync

show | set

show ntpsync

Use this operation to get status of ntpd

Synopsys

show ntpsync

---

set ntpsync

Use this operation to enable/disable ntpd

Synopsys

set ntpsync [ntpd_status=(false | true)]

Parameters

ntpd_status

ntpd status

---

passwordpolicy

Aug 18, 2015

Password Policy configuration

show | set

show passwordpolicy

Use this operation to get Password Policy details

Synopsys

show passwordpolicy [id=<string>]

Parameters

id

Id is system generated key

---

set passwordpolicy

Use this operation to modify Password Policy details

Synopsys

set passwordpolicy [enable_password_complexity=(false | true)] [minimum_password_length=<int>]

Parameters

enable_password_complexity

Enable user Password complexity

minimum_password_length

Minimum password length

---

prunepolicy

Aug 18, 2015

Prune Policy

show | set

show prunepolicy

Use this operation to get the prune policy to view number of days data to retain

Synopsys

show prunepolicy [policy_name=<string>]

Parameters

policy_name

Policy Name

---

set prunepolicy

Use this operation to modify the number of days data to retain

Synopsys

set prunepolicy data_to_keep_in_days=<int> [policy_name=<string>]

Parameters

data_to_keep_in_days

Number of days data to retain

This is a mandatory parameter.

policy_name

Policy Name

---

snmpmib

Aug 18, 2015

SNMP MIB Information

show | set

show snmpmib

Use this operation to get snmp mib information

Synopsys

show snmpmib [id=<string>]

Parameters

id

Id is system generated key

---

set snmpmib

Use this operation to modify snmp mib information

Synopsys

set snmpmib location=<string> name=<string> contact=<string> [custom_id=<string>]

Parameters

location

Physical location of appliance

This is a mandatory parameter.

name

Name for appliance

This is a mandatory parameter.

contact

Name of the administrator for appliance.

This is a mandatory parameter.

custom_id

Custom identification number for appliance

radiusserver

Aug 18, 2015

Radius Server configuration

show | delete | set | add

show radiusserver

Use this operation to get Radius server details

Synopsys

show radiusserver [id=<string>]

Parameters

id

Id is system generated key for all the radius servers

---

delete radiusserver

Use this operation to delete Radius server

Synopsys

delete radiusserver id=<string>

Parameters

id

Id is system generated key for all the radius servers

This is a mandatory parameter.

---

set radiusserver

Use this operation to modify Radius server

Synopsys

set radiusserver id=<string> ip_address=<ipaddress> name=<string> [port=<int>] [ip_vendor_id=<int>] [ip_attribute_type=<int>] [nas_id=<string>] [auth_timeout=<int>] [pwd_attribute_type=<int>] [accounting=(false | true)] [group_vendor_id=<int>] [group_attribute_type=<int>] [pwd_vendor_id=<int>] [default_authentication_group=<string>] [group_separator=<string>] [pass_encoding=<string>] [radius_key=<stringx>] [enable_nas_ip=(false | true)] [groups_prefix=<string>]

Parameters

id

Id is system generated key for all the radius servers

This is a mandatory parameter.

ip_address

IP Address of radius server

This is a mandatory parameter.

name

Name of radius server

This is a mandatory parameter.

port

Port number of radius server

ip_vendor_id

The vendor ID of the attribute in the RADIUS response which denotes the intranet IP

ip_attribute_type

The attribute type of the remote IP address attribute in a RADIUS response

nas_id

NAS ID

auth_timeout

The maximum number of seconds the system will wait for a response from the Radius server

pwd_attribute_type

The attribute type of the password attribute in a RADIUS response.

accounting

Enable accounting in the radius server

group_vendor_id

Vendor ID for RADIUS group extraction

group_attribute_type

Attribute type for RADIUS group extraction

pwd_vendor_id

Vendor ID of the password in the RADIUS response. Used to extract the user password

default_authentication_group

This is the default group that is chosen when the authentication succeeds in addition to extracted groups

group_separator

Group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction

pass_encoding

Enable password encoding in RADIUS packets send to the RADIUS server

radius_key

Key of radius server

enable_nas_ip

Enable NAS IP extraction

groups_prefix

Prefix string that precedes group names within a RADIUS attribute for RADIUS group extraction

---

add radiusserver

Use this operation to add Radius server

Synopsys

add radiusserver ip_address=<ipaddress> name=<string> radius_key=<stringx> [port=<int>] [ip_vendor_id=<int>] [ip_attribute_type=<int>] [nas_id=<string>] [auth_timeout=<int>] [pwd_attribute_type=<int>] [accounting=(false | true)] [group_vendor_id=<int>] [group_attribute_type=<int>] [pwd_vendor_id=<int>] [default_authentication_group=<string>] [group_separator=<string>] [pass_encoding=<string>] [enable_nas_ip=(false | true)] [groups_prefix=<string>]

Parameters

ip_address

IP Address of radius server

This is a mandatory parameter.

name

Name of radius server

This is a mandatory parameter.

radius_key

Key of radius server

This is a mandatory parameter.

port

Port number of radius server

ip_vendor_id

The vendor ID of the attribute in the RADIUS response which denotes the intranet IP

ip_attribute_type

The attribute type of the remote IP address attribute in a RADIUS response

nas_id

NAS ID

auth_timeout

The maximum number of seconds the system will wait for a response from the Radius server

pwd_attribute_type

The attribute type of the password attribute in a RADIUS response.

accounting

Enable accounting in the radius server

group_vendor_id

Vendor ID for RADIUS group extraction

group_attribute_type

Attribute type for RADIUS group extraction

pwd_vendor_id

Vendor ID of the password in the RADIUS response. Used to extract the user password

default_authentication_group

This is the default group that is chosen when the authentication succeeds in addition to extracted groups

group_separator

Group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction

pass_encoding

Enable password encoding in RADIUS packets send to the RADIUS server

enable_nas_ip

Enable NAS IP extraction

groups_prefix

Prefix string that precedes group names within a RADIUS attribute for RADIUS group extraction

rediscover

Aug 18, 2015

Inventory

show rediscover

Use this operation to start inventory of a given device. All devices if device IP Address is not specified.

Synopsys

show rediscover [device_ipaddress=<ipaddress>]

Parameters

device_ipaddress

Device IP Address

singlebundleimage

Aug 18, 2015

CBSDX Single Bundle Build File

show | delete

show singlebundleimage

Use this operation to get build file

Synopsys

show singlebundleimage [file_name=<string>]

Parameters

file_name

File Name

---

delete singlebundleimage

Use this operation to delete build file

Synopsys

delete singlebundleimage [file_name=<string>]

Parameters

file_name

File Name

---

singlebundleinfo

Aug 18, 2015

Single Bundle File Info

show singlebundleinfo

Use this operation to get build file

Synopsys

show singlebundleinfo

singlebundleupgrade

Aug 18, 2015

CBSDX Single Bundle Upgrade

do singlebundleupgrade custom

Use this operation to upgrade using single bundle image

Synopsys

do singlebundleupgrade custom [file_name=<string>]

Parameters

file_name

File Name

smsprofile

Aug 18, 2015

SMS profile

show | delete | set | add

show smsprofile

Use this operation to get sms profile.

Synopsys

show smsprofile [id=<string>]

Parameters

id

Id is system generated key for all the sms profile.

---

delete smsprofile

Use this operation to delete sms profile.

Synopsys

delete smsprofile id=<string>

Parameters

id

Id is system generated key for all the sms profile.

This is a mandatory parameter.

---

set smsprofile

Use this operation to modify sms profile.

Synopsys

set smsprofile id=<string> [to_list=<string>] [server_name=<string>] [profile_name=<string>]

Parameters

id

Id is system generated key for all the sms profile.

This is a mandatory parameter.

to_list

To list.

server_name

SMS server name

profile_name

Profile name for the sms setting.

---

add smsprofile

Use this operation to add sms profile.

Synopsys

add smsprofile to_list=<string> server_name=<string> profile_name=<string>

Parameters

to_list

To list.

This is a mandatory parameter.

server_name

SMS server name

This is a mandatory parameter.

profile_name

Profile name for the sms setting.

This is a mandatory parameter.

---

smsserver

Aug 18, 2015

SMS server properties

show | delete | set | add

show smsserver

Use this operation to get sms server details.

Synopsys

show smsserver [id=<string>]

Parameters

id

Id is system generated key for all the sms server

---

delete smsserver

Use this operation to delete sms server

Synopsys

delete smsserver id=<string>

Parameters

id

Id is system generated key for all the sms server

This is a mandatory parameter.

---

set smsserver

Use this operation to modify sms server

Synopsys

set smsserver id=<string> [is_ssl=(false | true)] [optional2_key=<string>] [to_separator=<string>] [to_key=<string>] [username_key=<string>] [message_word_separator=<string>] [optional_key=<string>] [type=<string>] [base_url=<string>] [message_key=<string>] [optional_val=<string>] [server_name=<string>] [optional2_val1=<string>] [password_val=<stringx>] [username_val=<string>] [password_key=<string>] [optional3_key=<string>] [optional3_val=<string>]

Parameters

id

Id is system generated key for all the sms server

This is a mandatory parameter.

is_ssl

Is SSL support configured.

optional2_key

Optional2 key for the sms server

to_separator

To list seperater for the sms server

to_key

To key for the sms server

username_key

Username key for the sms server

message_word_separator

Message Word Seperater for the sms server

optional_key

Optional1 key for the sms server

type

HTTP type supported for the sms server

base_url

Base URL for the sms server, without payload

message_key

Message key for the sms server

optional_val

Optional1 Val for the sms server

server_name

SMS server name

optional2_val1

Optional2 Val for the sms server

password_val

Password Val for the sms server

username_val

Username val for the sms server

password_key

Password key for the sms server

optional3_key

Optional3 key for the sms server

optional3_val

Optional3 Val for the sms server

---

add smsserver

Use this operation to add sms server

Synopsys

add smsserver to_key=<string> username_key=<string> type=<string> base_url=<string> message_key=<string> server_name=<string> password_val=<stringx> username_val=<string> password_key=<string> [is_ssl=(false | true)] [optional2_key=<string>] [to_separator=<string>] [message_word_separator=<string>] [optional_key=<string>] [optional_val=<string>] [optional2_val1=<string>] [optional3_key=<string>] [optional3_val=<string>]

Parameters

to_key

To key for the sms server

This is a mandatory parameter.

username_key

Username key for the sms server

This is a mandatory parameter.

type

HTTP type supported for the sms server

This is a mandatory parameter.

base_url

Base URL for the sms server, without payload

This is a mandatory parameter.

message_key

Message key for the sms server

This is a mandatory parameter.

server_name

SMS server name

This is a mandatory parameter.

password_val

Password Val for the sms server

This is a mandatory parameter.

username_val

Username val for the sms server

This is a mandatory parameter.

password_key

Password key for the sms server

This is a mandatory parameter.

is_ssl

Is SSL support configured.

optional2_key

Optional2 key for the sms server

to_separator

To list seperater for the sms server

message_word_separator

Message Word Seperater for the sms server

optional_key

Optional1 key for the sms server

optional_val

Optional1 Val for the sms server

optional2_val1

Optional2 Val for the sms server

optional3_key

Optional3 key for the sms server

optional3_val

Optional3 Val for the sms server

smtpserver

Aug 18, 2015

SMTP server properties

show | delete | set | add

show smtpserver

Use this operation to get smtp server details.

Synopsys

show smtpserver [id=<string>]

Parameters

id

Id is system generated key for all the smtp server

---

delete smtpserver

Use this operation to delete smtp server

Synopsys

delete smtpserver id=<string>

Parameters

id

Id is system generated key for all the smtp server

This is a mandatory parameter.

---

set smtpserver

Use this operation to modify smtp server

Synopsys

set smtpserver id=<string> [is_ssl=(false | true)] [port=<int>] [server_name=<internethost>] [username=<string>] [is_auth=(false | true)] [password=<stringx>]

Parameters

id

Id is system generated key for all the smtp server

This is a mandatory parameter.

is_ssl

Is this smtp server is SSL support configured.

port

SMTP Server port address.

server_name

SMTP server name

username

Username for the smtp server

is_auth

Is authentication enabled for this smtp server

password

Password for the smtp server

---

add smtpserver

Use this operation to add smtp server

Synopsys

add smtpserver server_name=<internethost> [is_ssl=(false | true)] [port=<int>] [username=<string>] [is_auth=(false | true)] [password=<stringx>]

Parameters

server_name

SMTP server name

This is a mandatory parameter.

is_ssl

Is this smtp server is SSL support configured.

port

SMTP Server port address.

username

Username for the smtp server

is_auth

Is authentication enabled for this smtp server

password

Password for the smtp server

snmpalarm

Aug 18, 2015

SNMP Alarm Configurations

show | set

show snmpalarm

Use this operation to get snmp alarm configuration

Synopsys

show snmpalarm [name=<string>]

Parameters

name

Alarm Name

---

set snmpalarm

Use this operation to modify snmp alarm configuration

Synopsys

set snmpalarm [name=<string>] [enable=(false | true)] [severity=<string>]

Parameters

name

Alarm Name

enable

Enable Alarm

severity

Alarm severity. Supported values: Critical, Major, Minor, Warning, Informational

---

snmpinfo

Aug 18, 2015

SNMP Information

show | set

show snmpinfo

Use this operation to get snmp information

Synopsys

show snmpinfo

---

set snmpinfo

Use this operation to modify snmp information

Synopsys

set snmpinfo engine_id=<string>

Parameters

engine_id

SNMP EngineID

This is a mandatory parameter.

---

snmpmanager

Aug 18, 2015

SNMP Agent Manager configuration

show | delete | set | add

show snmpmanager

Use this operation to get SNMP Manager details

Synopsys

show snmpmanager [snmp_manager=<internethost>]

Parameters

snmp_manager

Manager IPAddress

---

delete snmpmanager

Use this operation to delete SNMP Manager

Synopsys

delete snmpmanager snmp_manager=<internethost>

Parameters

snmp_manager

Manager IPAddress

This is a mandatory parameter.

---

set snmpmanager

Use this operation to modify SNMP Manager

Synopsys

set snmpmanager snmp_manager=<internethost> community=<string>

Parameters

snmp_manager

Manager IPAddress

This is a mandatory parameter.

community

Community Name

This is a mandatory parameter.

---

add snmpmanager

Use this operation to add SNMP Manager

Synopsys

add snmpmanager snmp_manager=<internethost> community=<string>

Parameters

snmp_manager

Manager IPAddress

This is a mandatory parameter.

community

Community Name

This is a mandatory parameter.

---

snmptrap

Aug 18, 2015

SNMP Trap Destinations

show | delete | set | add

show snmptrap

Use this operation to get snmp trap destination details

Synopsys

show snmptrap [dest_server=<internethost>]

Parameters

dest_server

Trap Destination Server Address

---

delete snmptrap

Use this operation to delete snmp trap destination

Synopsys

delete snmptrap dest_server=<internethost>

Parameters

dest_server

Trap Destination Server Address

This is a mandatory parameter.

---

set snmptrap

Use this operation to modify snmp trap destination

Synopsys

set snmptrap dest_server=<internethost> [user_name=<string...>] [community=<string>] [dest_port=<int>] [version=<string>]

Parameters

dest_server

Trap Destination Server Address

This is a mandatory parameter.

user_name

Name of SNMP Trap User

community

Community Name

dest_port

Destination Port

version

SNMP version

---

add snmptrap

Use this operation to add snmp trap destination

Synopsys

add snmptrap dest_server=<internethost> [user_name=<string...>] [community=<string>] [dest_port=<int>] [version=<string>]

Parameters

dest_server

Trap Destination Server Address

This is a mandatory parameter.

user_name

Name of SNMP Trap User

community

Community Name

dest_port

Destination Port

version

SNMP version

---

snmpuser

Aug 18, 2015

SNMP User

show | delete | set | add

show snmpuser

Use this operation to get SNMP User details

Synopsys

show snmpuser [name=<string>]

Parameters

name

Name of SNMP User

---

delete snmpuser

Use this operation to delete SNMP User

Synopsys

delete snmpuser name=<string>

Parameters

name

Name of SNMP User

This is a mandatory parameter.

---

set snmpuser

Use this operation to modify SNMP User

Synopsys

set snmpuser security_level=<int> name=<string> [view_name=<string>] [auth_protocol=<int>] [privacy_protocol=<int>] [auth_password=<stringx>] [privacy_password=<stringx>]

Parameters

security_level

Security Level of SNMP User. Values: 0: noAuthNoPriv, 1: authNoPriv, 2: authPriv

This is a mandatory parameter.

name

Name of SNMP User

This is a mandatory parameter.

view_name

SNMP View Name attached to the SNMP User

auth_protocol

Authentication Protocol of SNMP User. Values: 0:noValue, 1: MD5, 2: SHA1

privacy_protocol

Privacy Protocol of SNMP User. Values: 0:noValue, 1: DES, 2: AES

auth_password

Authentication Password of SNMP User

privacy_password

Privacy Password of SNMP User

---

add snmpuser

Use this operation to add SNMP User

Synopsys

add snmpuser security_level=<int> name=<string> [view_name=<string>] [auth_protocol=<int>] [privacy_protocol=<int>] [auth_password=<stringx>] [privacy_password=<stringx>]

Parameters

security_level

Security Level of SNMP User. Values: 0: noAuthNoPriv, 1: authNoPriv, 2: authPriv

This is a mandatory parameter.

name

Name of SNMP User

This is a mandatory parameter.

view_name

SNMP View Name attached to the SNMP User

auth_protocol

Authentication Protocol of SNMP User. Values: 0:noValue, 1: MD5, 2: SHA1

privacy_protocol

Privacy Protocol of SNMP User. Values: 0:noValue, 1: DES, 2: AES

auth_password

Authentication Password of SNMP User

privacy_password

Privacy Password of SNMP User

snmpview

Aug 18, 2015

SNMP view

show | delete | set | add

show snmpview

Use this operation to get SNMP View details

Synopsys

show snmpview [name=<string>]

Parameters

name

Name of SNMP view

---

delete snmpview

Use this operation to delete SNMP View

Synopsys

delete snmpview name=<string>

Parameters

name

Name of SNMP view

This is a mandatory parameter.

---

set snmpview

Use this operation to modify SNMP View

Synopsys

set snmpview name=<string> [subtree=<string>] [type=(false | true)]

Parameters

name

Name of SNMP view

This is a mandatory parameter.

subtree

Subtree associated with the SNMP view

type

Include or Exclude the associated subtree . Values. true:Include, false: Exclude

---

add snmpview

Use this operation to add SNMP View

Synopsys

add snmpview name=<string> [subtree=<string>] [type=(false | true)]

Parameters

name

Name of SNMP view

This is a mandatory parameter.

subtree

Subtree associated with the SNMP view

type

Include or Exclude the associated subtree . Values. true:Include, false: Exclude

---

sslcertfile

Aug 18, 2015

SSL certificate File

show | delete

show sslcertfile

Use this operation to get ssl certificate file

Synopsys

show sslcertfile [file_name=<string>]

Parameters

file_name

File Name

---

delete sslcertfile

Use this operation to delete ssl certificate file

Synopsys

delete sslcertfile file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

sslcertificate

Aug 18, 2015

Install SSL certificate on Management Service

show | add

show sslcertificate

Use this operation to get certificate on Management Service

Synopsys

show sslcertificate

---

add sslcertificate

Use this operation to install certificate on Management Service

Synopsys

add sslcertificate ssl_certificate=<string> [status=<string>] [subject=<string>] [ssl_key=<string>] [valid_from=<string>] [days_to_expiry=<int>] [public_key_size=<int>] [public_key_algorithm=<string>] [password=<stringx>] [version=<string>] [serial_number=<int>] [signature_algorithm=<string>] [issuer=<string>] [valid_to=<string>]

Parameters

ssl_certificate

Certificate

This is a mandatory parameter.

status

Tells whether the certificate is still valid or not

subject

Subject

ssl_key

Key

valid_from

Valid From

days_to_expiry

Days before SSL certificate expires

public_key_size

Public Key Size

public_key_algorithm

Public Key Algorithm

password

The pass-phrase that was used to encrypt the private-key.

version

Version

serial_number

Serial Number

signature_algorithm

Signature Algorithm

issuer

Issuer

valid_to

Valid To

sslkeyfile

Aug 18, 2015

SSL key File

show | delete

show sslkeyfile

Use this operation to get ssl key file

Synopsys

show sslkeyfile [file_name=<string>]

Parameters

file_name

File Name

---

delete sslkeyfile

Use this operation to delete ssl key file

Synopsys

delete sslkeyfile file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

sslsettings

Aug 18, 2015

SSL Settings

show | set

show sslsettings

Use this operation to get ssl settings

Synopsys

show sslsettings

---

set sslsettings

Use this operation to modify ssl settings

Synopsys

set sslsettings [sslv3=(false | true)] [sslreneg=(false | true)] [tlsv1=(false | true)] [tlsv1_2=(false | true)] [tlsv1_1=(false | true)]

Parameters

sslv3

Enable SSLv3

sslreneg

Enable SSL Renegotiation

tlsv1

Enable TLSv1

tlsv1_2

Enable TLSv1.2

tlsv1_1

Enable TLSv1.1

---

sslv3Setting

Aug 18, 2015

SSLV3 Setting

show | set

show sslv3Setting

Use this operation to get sslv3 settings

Synopsys

show sslv3Setting

---

set sslv3Setting

Use this operation to modify sslv3 settings

Synopsys

set sslv3Setting [enable=(false | true)]

Parameters

enable

Secure Access only

---

syslogparameters

Aug 18, 2015

Syslog Parameters

show | set

show syslogparameters

Use this operation to get the syslog parameters

Synopsys

show syslogparameters [id=<string>]

Parameters

id

Id is system generated key

---

set syslogparameters

Use this operation to modify the syslog parameters

Synopsys

set syslogparameters [timezone=<string>] [date_format=<string>]

Parameters

timezone

Timezone to be used in the syslog message

date_format

Format of date to be added in the syslog message

---

syslogserver

Aug 18, 2015

Syslog Server

show | delete | set | add

show syslogserver

Use this operation to get all the syslog servers

Synopsys

show syslogserver [name=<string>]

Parameters

name

Syslog server name

---

delete syslogserver

Use this operation to delete a syslog server

Synopsys

delete syslogserver [name=<string>]

Parameters

name

Syslog server name

---

set syslogserver

Use this operation to modify a syslog server

Synopsys

set syslogserver [log_level_all=(false | true)] [log_level_error=(false | true)] [log_level_none=(false | true)] [log_level_warning=(false | true)] [port=<int>] [log_level_critical=(false | true)] [log_level_info=(false | true)] [name=<string>]

Parameters

log_level_all

Send logs of all levels to this syslog server

log_level_error

Send logs of level error to this syslog server

log_level_none

Send no logs to this syslog server

log_level_warning

Send logs of level warning to this syslog server

port

Syslog server port

log_level_critical

Send logs of level critical to this syslog server

log_level_info

Send logs of level info to this syslog server

name

Syslog server name

---

add syslogserver

Use this operation to add a syslog server

Synopsys

add syslogserver port=<int> ip_address=<ipaddress> name=<string> [log_level_all=(false | true)] [log_level_info=(false | true)] [log_level_none=(false | true)] [log_levels=<string>] [log_level_warning=(false | true)] [log_level_critical=(false | true)] [log_level_error=(false | true)]

Parameters

port

Syslog server port

This is a mandatory parameter.

ip_address

Syslog server IP address

This is a mandatory parameter.

name

Syslog server name

This is a mandatory parameter.

log_level_all

Send logs of all levels to this syslog server

log_level_info

Send logs of level info to this syslog server

log_level_none

Send no logs to this syslog server

log_levels

Set of all log levels at which messages are sent to this syslog server

log_level_warning

Send logs of level warning to this syslog server

log_level_critical

Send logs of level critical to this syslog server

log_level_error

Send logs of level error to this syslog server

systembackuprestore

Aug 18, 2015

Backup

show | do factory_default

show systembackuprestore

Use this operation to get backup/restore information

Synopsys

show systembackuprestore [file_name=<string>]

Parameters

file_name

File Name

---

do systembackuprestore factory_default

Use this operation to Restore factory default

Synopsys

do systembackuprestore factory_default [reset_type=<int>]

Parameters

reset_type

Reset Type [0: Reset (Without Network Configuration), 1: Reset (With Network Configuration), 2: Appliance Reset, 3: Appliance Restore, 4: Instance Restore, 5: Backup]

---

tenant

Aug 18, 2015

Tenant on SDX Platform

show | delete | set | add

show tenant

Use this operation to get tenants.

Synopsys

show tenant [id=<string>]

Parameters

id

Id is system generated key for all the Tenants

---

delete tenant

Use this operation to delete a tenant.

Synopsys

delete tenant id=<string>

Parameters

id

Id is system generated key for all the Tenants

This is a mandatory parameter.

---

set tenant

Use this operation to modify a tenant.

Synopsys

set tenant id=<string> [user_name=<string>] [system_resource=<tenant_system_resource>] [auth_servers=<tenant_auth_server...>] [name=<string>] [company_info=<tenant_company_info>] [password=<stringx>] [network_pools=<tenant_network_pool...>] [parent_id=<string>]

Parameters

id

Id is system generated key for all the Tenants

This is a mandatory parameter.

user_name

User Name for tenant

system_resource

Tenant System Resource

auth_servers

Tenant Authentication Servers

name

Name of the Tenant

company_info

Tenant Company Information

password

Password

network_pools

Tenant Network Pools

parent_id

Tenant ID of the parent Tenant.

---

add tenant

Use this operation to add a tenant.

Synopsys

add tenant user_name=<string> password=<stringx> parent_id=<string> [system_resource=<tenant_system_resource>] [auth_servers=<tenant_auth_server...>] [name=<string>] [company_info=<tenant_company_info>] [network_pools=<tenant_network_pool...>]

Parameters

user_name

User Name for tenant

This is a mandatory parameter.

password

Password

This is a mandatory parameter.

parent_id

Tenant ID of the parent Tenant.

This is a mandatory parameter.

system_resource

Tenant System Resource

auth_servers

Tenant Authentication Servers

name

Name of the Tenant

company_info

Tenant Company Information

network_pools

Tenant Network Pools

systemgroup

Aug 18, 2015

System Groups

show | delete | set | add

show systemgroup

Use this operation to get system groups

Synopsys

show systemgroup [id=<string>]

Parameters

id

Id is system generated key for all the system groups

---

delete systemgroup

Use this operation to delete system group(s)

Synopsys

delete systemgroup id=<string>

Parameters

id

Id is system generated key for all the system groups

This is a mandatory parameter.

---

set systemgroup

Use this operation to modify system group

Synopsys

set systemgroup id=<string> [name=<string>] [session_timeout=<int>] [tenant_id=<string>] [session_timeout_unit=<string>] [enable_session_timeout=(false | true)] [permission=<string>] [users=<string...>]

Parameters

id

Id is system generated key for all the system groups

This is a mandatory parameter.

name

Group Name

session_timeout

Session timeout for the Group

tenant_id

Id of the tenant

session_timeout_unit

Session timeout unit for the Group

enable_session_timeout

Enables session timeout for group

permission

Permission for the group (admin/read-only)

users

Users belong to the group

---

add systemgroup

Use this operation to add system group

Synopsys

add systemgroup name=<string> permission=<string> [session_timeout=<int>] [tenant_id=<string>] [session_timeout_unit=<string>] [enable_session_timeout=(false | true)] [users=<string...>]

Parameters

name

Group Name

This is a mandatory parameter.

permission

Permission for the group (admin/read-only)

This is a mandatory parameter.

session_timeout

Session timeout for the Group

tenant_id

Id of the tenant

session_timeout_unit

Session timeout unit for the Group

enable_session_timeout

Enables session timeout for group

users

Users belong to the group

---

systemimage

Aug 18, 2015

System Build File

show | delete

show systemimage

Use this operation to get build file

Synopsys

show systemimage [file_name=<string>]

Parameters

file_name

File Name

---

delete systemimage

Use this operation to delete build file

Synopsys

delete systemimage file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

systemsession

Aug 18, 2015

Client Session

show | delete

show systemsession

Use this operation to get client sessions

Synopsys

show systemsession [id=<string>]

Parameters

id

Id is system generated key for all the client sessions

---

delete systemsession

Kill client session by providing id

Synopsys

delete systemsession id=<string>

Parameters

id

Id is system generated key for all the client sessions

This is a mandatory parameter.

---

systemsettings

Aug 18, 2015

System Settings

show | set

show systemsettings

Use this operation to get system settings

Synopsys

show systemsettings [id=<string>]

Parameters

id

Id is system generated key

---

set systemsettings

Use this operation to modify system settings

Synopsys

set systemsettings [is_metering_enabled=(false | true)] [secure_access_only=(false | true)] [session_timeout=<int>] [session_timeout_unit=<string>] [enable_session_timeout=(false | true)] [basicauth=(false | true)] [svm_ns_comm=<string>] [act_id=<string>]

Parameters

is_metering_enabled

Enable Metering for NS VPX's on SDX

secure_access_only

Secure Access only

session_timeout

Session timeout for the system

session_timeout_unit

Session timeout unit for the system

enable_session_timeout

Enables session timeout feature

basicauth

Allow Basic Authentication Protocol

svm_ns_comm

Communication with NetScaler

act_id

Activity Id

systemstatus

Aug 18, 2015

System Status

show | do reboot

show systemstatus

Use this operation to get system status

Synopsys

show systemstatus

---

do systemstatus reboot

Use this operation to reboot

Synopsys

do systemstatus reboot

---

systemupgrade

Aug 18, 2015

System Upgrade

do systemupgrade custom

Use this operation to upgrade

Synopsys

do systemupgrade custom [image_name=<string>]

Parameters

image_name

image_name

systemuser

Aug 18, 2015

System User

show | delete | set | add

show systemuser

Use this operation to get system users

Synopsys

show systemuser [id=<string>]

Parameters

id

Id is system generated key for all the system users

---

delete systemuser

Use this operation to delete system user(s)

Synopsys

delete systemuser id=<string>

Parameters

id

Id is system generated key for all the system users

This is a mandatory parameter.

---

set systemuser

Use this operation to modify system user

Synopsys

set systemuser id=<string> [external_authentication=(false | true)] [name=<string>] [session_timeout=<int>] [session_timeout_unit=<string>] [enable_session_timeout=(false | true)] [permission=<string>] [password=<stringx>] [encrypted=(false | true)] [groups=<string...>]

Parameters

id

Id is system generated key for all the system users

This is a mandatory parameter.

external_authentication

Enable external authentication

name

User Name

session_timeout

Session timeout for the user

session_timeout_unit

Session timeout unit for the user

enable_session_timeout

Enables session timeout for user

permission

Actions that this user is authorized to perform

password

Password

encrypted

Provide encrypted password

groups

Groups to which user belongs

---

add systemuser

Use this operation to add system user

Synopsys

add systemuser name=<string> password=<stringx> [external_authentication=(false | true)] [session_timeout=<int>] [session_timeout_unit=<string>] [enable_session_timeout=(false | true)] [permission=<string>] [encrypted=(false | true)] [groups=<string...>]

Parameters

name

User Name

This is a mandatory parameter.

password

Password

This is a mandatory parameter.

external_authentication

Enable external authentication

session_timeout

Session timeout for the user

session_timeout_unit

Session timeout unit for the user

enable_session_timeout

Enables session timeout for user

permission

Actions that this user is authorized to perform

encrypted

Provide encrypted password

groups

Groups to which user belongs

tacacsserver

Aug 18, 2015

TACACS Server configuration

show | delete | set | add

show tacacsserver

Use this operation to get TACACS server details

Synopsys

show tacacsserver [id=<string>]

Parameters

id

Id is system generated key for all the TACACS servers

---

delete tacacsserver

Use this operation to delete TACACS server

Synopsys

delete tacacsserver id=<string>

Parameters

id

Id is system generated key for all the TACACS servers

This is a mandatory parameter.

---

set tacacsserver

Use this operation to modify TACACS server

Synopsys

set tacacsserver id=<string> ip_address=<ipaddress> name=<string> [port=<int>] [tacacs_key=<stringx>] [auth_timeout=<int>] [accounting=(false | true)]

Parameters

id

Id is system generated key for all the TACACS servers

This is a mandatory parameter.

ip_address

IP Address of TACACS server

This is a mandatory parameter.

name

Name of TACACS server

This is a mandatory parameter.

port

port number of TACACS server

tacacs_key

Key shared between the TACACS+ server and clients

auth_timeout

The maximum number of seconds the system will wait for a response from the TACACS server

accounting

Enable accounting in the tacacs server

---

add tacacsserver

Use this operation to add TACACS server

Synopsys

add tacacsserver ip_address=<ipaddress> tacacs_key=<stringx> name=<string> [port=<int>] [auth_timeout=<int>] [accounting=(false | true)]

Parameters

ip_address

IP Address of TACACS server

This is a mandatory parameter.

tacacs_key

Key shared between the TACACS+ server and clients

This is a mandatory parameter.

name

Name of TACACS server

This is a mandatory parameter.

port

port number of TACACS server

auth_timeout

The maximum number of seconds the system will wait for a response from the TACACS server

accounting

Enable accounting in the tacacs server

---

techsupport

Aug 18, 2015
Technical Support

do ApplianceIncludingInstances | do ManagementService | show | do ManagementServiceIncludingInstances | do XenServer | delete | do ManagementServiceAndXen

do techsupport ApplianceIncludingInstances

Use this operation to generate technical support archive

Synopsys

do techsupport ApplianceIncludingInstances [vpx_list_for_techsupport=<string...>]

Parameters

vpx_list_for_techsupport

List of VPX for which the techsupport is required (Applicable for only : ManagementServiceIncludingInstances and ApplianceIncludingInstances)

---

do techsupport ManagementService

Use this operation to generate technical support archive

Synopsys

do techsupport ManagementService [file_name=<string>]

Parameters

file_name

Technical support File Name

---

show techsupport

Use this operation to get technical support file

Synopsys

show techsupport [file_name=<string>]

Parameters

file_name

Technical support File Name

do techsupport ManagementServiceIncludingInstances

Use this operation to generate technical support archive

Synopsys

do techsupport ManagementServiceIncludingInstances [vpx_list_for_techsupport=<string...>]

Parameters

vpx_list_for_techsupport

List of VPX for which the techsupport is required (Applicable for only : ManagementServiceIncludingInstances and ApplianceIncludingInstances)

---

do techsupport XenServer

Use this operation to generate technical support archive

Synopsys

do techsupport XenServer [file_name=<string>]

Parameters

file_name

Technical support File Name

---

delete techsupport

Use this operation to delete technical support file

Synopsys

delete techsupport file_name=<string>

Parameters

file_name

Technical support File Name

This is a mandatory parameter.

---

do techsupport ManagementServiceAndXen

Use this operation to generate technical support archive

Synopsys

do techsupport ManagementServiceAndXen [file_name=<string>]

Parameters

file_name

Technical support File Name

timezone

Aug 18, 2015

Current timezone

show | set

show timezone

Use this operation to get the current time zone

Synopsys

show timezone

---

set timezone

Use this operation to modify current time zone

Synopsys

set timezone [timezone=<string>]

Parameters

timezone

Timezone

---

userlockoutpolicy

Aug 18, 2015

User Lockout Policy configuration

show | set

show userlockoutpolicy

Use this operation to get User Lockout Policy details

Synopsys

show userlockoutpolicy [id=<string>]

Parameters

id

Id is system generated key

---

set userlockoutpolicy

Use this operation to modify User Lockout Policy details

Synopsys

set userlockoutpolicy [user_lockout_interval=<int>] [invalid_logins=<int>] [enable_user_lockout=(false | true)]

Parameters

user_lockout_interval

User lockout Interval in secoonds

invalid_logins

No of invalid logins for User lockout

enable_user_lockout

Enable user User lockout feature

---

vlandetails

Aug 18, 2015

VLAN details

show vlandetails

Use this operation to get vlan details

Synopsys

show vlandetails [vlan_id=<int>]

Parameters

vlan_id

VLAN ID

vlansummary

Aug 18, 2015

VLAN summary

show vlansummary

Use this operation to get vlan summary

Synopsys

show vlansummary

vmdevice

Aug 18, 2015

VM Device

show vmdevice

Use this operation to get VM Instance

Synopsys

show vmdevice [id=<string>]

Parameters

id

Id is system generated key for all the VM Instances

NetScaler

Aug 18, 2015

The entities on which you can perform NetScaler SDX CLI operations:

- ns - NetScaler
- nsdocimage - NetScaler Documentation File
- nsimage - NetScaler Build File
- nssslcertfile - NS SSL certificate File
- nssslcertkey - SSL certificate on NetScaler
- nssslcertkeypolicy - NetScaler SSL Cert-Key Polling Policy
- nssslkeyfile - NS SSL key File
- nsupgrade - Upgrade NetScaler

ns

Aug 18, 2015
NetScaler

do stop | show | do start | do reboot | delete | set | do force_reboot | add | do force_stop

do ns stop

Use this operation to stop NetScaler Instance

Synopsys

do ns stop [id=<string>]

Parameters

id

Id is system generated key for all the NetScaler Instances

---

show ns

Use this operation to get NetScaler Instance

Synopsys

show ns [id=<string>] [name=<string>]

Parameters

id

Id is system generated key for all the NetScaler Instances

name

Name of managed device

---

do ns start

Use this operation to start NetScaler Instance

Synopsys

do ns start [id=<string>]

Parameters

id

Id is system generated key for all the NetScaler Instances

---

do ns reboot

Use this operation to reboot NetScaler Instance

Synopsys

do ns reboot [id=<string>]

Parameters

id

Id is system generated key for all the NetScaler Instances

---

delete ns

Use this operation to delete NetScaler Instances

Synopsys

delete ns id=<string>

Parameters

id

Id is system generated key for all the NetScaler Instances

This is a mandatory parameter.

---

set ns

Use this operation to modify NetScaler Instance

Synopsys

set ns id=<string> [name=<string>] [ip_address=<ipaddress>] [netmask=<ipaddress>] [gateway=<ipaddress>] [license=<string>] [admin_profile_name=<string>] [description=<string>] [vm_memory_total=<doublelong>] [num_of_ssl_chips=<int>] [throughput=<doublelong>] [pps=<doublelong>] [number_of_cores=<int>] [reboot_vm_on_cpu_change=(false | true)] [password=<stringx>] [cmd_policy=<string>] [l2_enabled=(false | true)] [if_0_1=(false | true)] [if_0_2=(false | true)] [la_mgmt=(false | true)] [vlan_id_0_1=<int>] [vlan_id_0_2=<int>] [network_interfaces=<network_interface...>] [nsvlan_id=<int>] [vlan_type=<int>] [nsvlan_tagged=(false | true)] [nsvlan_interfaces=<string...>]

Parameters

id

Id is system generated key for all the NetScaler Instances

This is a mandatory parameter.

name

Name of managed device

ip_address

IP Address for this managed device

netmask

Netmask of managed device

gateway

Default Gateway of managed device

license

Feature License for NetScaler Instance, needs to be set while provisioning (standard, enterprise, platinum)

admin_profile_name

Device Profile Name that is attached with this managed device

description

Description of managed device

vm_memory_total

Total Memory of VM Instance in MB

num_of_ssl_chips

Assign number of ssl virtual functions to VM Instance

throughput

Assign throughput in Mbps to VM Instance

pps

Assign packets per seconds to NetScaler Instance

number_of_cores

Number of cores that are assigned to VM Instance

reboot_vm_on_cpu_change

Reboot VMs on CPU change during resource allocation

password

Password for specified user on NetScaler Instance

cmd_policy

true if you want to allow shell/sftp/scp access to NetScaler Instance administrator

l2_enabled

L2mode status of VM Instance

if_0_1

Network 0/1 on VM Instance

if_0_2

Network 0/2 on VM Instance

la_mgmt

Bond consisting of management ports on VM Instance

vlan_id_0_1

VLAN id for the management interface 0/1

vlan_id_0_2

VLAN id for the management interface 0/2

network_interfaces

Network Interfaces

nsvlan_id

VLAN Id

vlan_type

VLAN Type, NS or L2 VLAN

nsvlan_tagged

NSVLAN Tagged

nsvlan_interfaces

VLAN Interfaces

---

do ns force_reboot

Use this operation to force reboot NetScaler Instance

Synopsys

do ns force_reboot [id=<string>]

Parameters

id

Id is system generated key for all the NetScaler Instances

---

add ns

Use this operation to add NetScaler Instance

Synopsys

add ns ip_address=<ipaddress> [gateway=<ipaddress>] [l2_enabled=(false | true)] [nsvlan_interfaces=<string...>] [pps=<doublelong>] [throughput=<doublelong>] [la_mgmt=(false | true)] [nsvlan_tagged=(false | true)] [license=<string>] [username=<string>] [cmd_policy=<string>] [name=<string>] [number_of_cores=<int>] [vlan_id_0_1=<int>] [if_0_1=(false | true)] [netmask=<ipaddress>] [vlan_id_0_2=<int>] [description=<string>] [if_0_2=(false | true)] [network_interfaces=<network_interface...>] [reboot_vm_on_cpu_change=(false | true)] [vlan_type=<int>] [xva_file_name=<string>] [password=<stringx>] [vm_memory_total=<doublelong>] [nsvlan_id=<int>]

Parameters

ip_address

IP Address for this managed device

This is a mandatory parameter.

gateway

Default Gateway of managed device

l2_enabled

L2mode status of VM Instance

nsvlan_interfaces

VLAN Interfaces

pps

Assign packets per seconds to NetScaler Instance

throughput

Assign throughput in Mbps to VM Instance

la_mgmt

Bond consisting of management ports on VM Instance

nsvlan_tagged

NSVLAN Tagged

license

Feature License for NetScaler Instance, needs to be set while provisioning (standard, enterprise, platinum)

username

User Name (except nsroot) to be configured on NetScaler Instance

cmd_policy

true if you want to allow shell/sftp/scp access to NetScaler Instance administrator

name

Name of managed device

number_of_cores

Number of cores that are assigned to VM Instance

vlan_id_0_1

VLAN id for the management interface 0/1

if_0_1

Network 0/1 on VM Instance

netmask

Netmask of managed device

vlan_id_0_2

VLAN id for the management interface 0/2

description

Description of managed device

if_0_2

Network 0/2 on VM Instance

network_interfaces

Network Interfaces

reboot_vm_on_cpu_change

Reboot VMs on CPU change during resource allocation

vlan_type

VLAN Type, NS or L2 VLAN

xva_file_name

Image Name, This parameter is used while provisioning VM Instance with XVA image, template_name is given priority if provided along with image_name

password

Password for specified user on NetScaler Instance

vm_memory_total

Total Memory of VM Instance in MB

nsvlan_id

VLAN Id

---

do ns force_stop

Use this operation to force stop NetScaler Instance

Synopsys

do ns force_stop [id=<string>]

Parameters

id

Id is system generated key for all the NetScaler Instances

---

nsdocimage

Aug 18, 2015

NetScaler Documentation File

show | delete

show nsdocimage

Use this operation to get NetScaler Documentation file

Synopsys

show nsdocimage [file_name=<string>]

Parameters

file_name

File Name

---

delete nsdocimage

Use this operation to delete NetScaler Documentation file

Synopsys

delete nsdocimage file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

nsimage

Aug 18, 2015
NetScaler Build File

show | delete

show nsimage

Use this operation to get NetScaler build file

Synopsys

show nsimage [file_name=<string>]

Parameters

file_name

File Name

---

delete nsimage

Use this operation to delete NetScaler build file

Synopsys

delete nsimage file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

nssslcertfile

Aug 18, 2015

NS SSL certificate File

show | delete

show nssslcertfile

Use this operation to get ns ssl certificate file

Synopsys

show nssslcertfile [file_name=<string>]

Parameters

file_name

File Name

---

delete nssslcertfile

Use this operation to delete ns ssl certificate file

Synopsys

delete nssslcertfile file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

nssslcertkey

Aug 18, 2015

SSL certificate on NetScaler

show | delete | set | add | do gen_csr

show nssslcertkey

Use this operation to get certificates on NetScaler Instance(s)

Synopsys

show nssslcertkey [id=<string>]

Parameters

id

Id is system generated key for all ssl cert-keys entries. For download operation "id" must be provided in the format <ns_ip_address>_<certkeypair_name>.tgz

---

delete nssslcertkey

Use this operation to delete certificates on NetScaler Instance(s)

Synopsys

delete nssslcertkey id=<string>

Parameters

id

Id is system generated key for all ssl cert-keys entries. For download operation "id" must be provided in the format <ns_ip_address>_<certkeypair_name>.tgz

This is a mandatory parameter.

---

set nssslcertkey

Use this operation to modify certificates on NetScaler Instance(s)

Synopsys

set nssslcertkey id=<string> [ssl_certificate=<string>] [ssl_key=<string>] [cert_format=<string>] [password=<stringx>] [save_config=(false | true)] [no_domain_check=(false | true)]

Parameters

id

Id is system generated key for all ssl cert-keys entries. For download operation "id" must be provided in the format <ns_ip_address>_<certkeypair_name>.tgz

This is a mandatory parameter.

ssl_certificate

Certificate

ssl_key

Key

cert_format

Certificate Format

password

The pass-phrase that was used to encrypt the private-key.

save_config

true, if save config is required

no_domain_check

Specify this option to override the check for matching domain names during certificate update operation

---

add nssslcertkey

Use this operation to install certificates on NetScaler Instance(s)

Synopsys

add nssslcertkey ssl_certificate=<string> certkeypair_name=<string> ns_ip_address_arr=<ipaddress...> [ssl_key=<string>] [cert_format=<string>] [password=<stringx>] [save_config=(false | true)]

Parameters

ssl_certificate

Certificate

This is a mandatory parameter.

certkeypair_name

Cert Key Pair Name

This is a mandatory parameter.

ns_ip_address_arr

List of NetScaler IP Address

This is a mandatory parameter.

ssl_key

Key

cert_format

Certificate Format

password

The pass-phrase that was used to encrypt the private-key.

save_config

true, if save config is required

---

do nssslcertkey gen_csr

Use this operation to generate CSR for the certificate

Synopsys

do nssslcertkey gen_csr [id=<string>]

Parameters

id

Id is system generated key for all ssl cert-keys entries. For download operation "id" must be provided in the format <ns_ip_address>_<certkeypair_name>.tgz

---

nssslcertkeypolicy

Aug 18, 2015

NetScaler SSL Cert-Key Polling Policy

do do_poll | show | set

do nssslcertkeypolicy do_poll

Use this operation to poll all SSL certificates from all NetScalers and update the database

Synopsys

do nssslcertkeypolicy do_poll

---

show nssslcertkeypolicy

Use this operation to get the polling frequency of the NetScaler SSL certificates

Synopsys

show nssslcertkeypolicy

---

set nssslcertkeypolicy

Use this operation to set the polling frequency of the NetScaler SSL certificates

Synopsys

set nssslcertkeypolicy [polling_interval=<int>] [interval_unit=<string>]

Parameters

polling_interval

Frequency of polling in minutes

interval_unit

Frequency unit (Minutes)

---

nssslkeyfile

Aug 18, 2015

NS SSL key File

show | delete

show nssslkeyfile

Use this operation to get ns ssl key file

Synopsys

show nssslkeyfile [file_name=<string>]

Parameters

file_name

File Name

---

delete nssslkeyfile

Use this operation to delete ns ssl key file

Synopsys

delete nssslkeyfile file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

nsupgrade

Aug 18, 2015

Upgrade NetScaler

do nsupgrade custom

Use this operation to upgrade NetScaler

Synopsys

do nsupgrade custom [image_name=<string>] [doc_file=<string>] [ns_ip_address_arr=<ipaddress...>]

Parameters

image_name

image_name

doc_file

Documentation File Name

ns_ip_address_arr

List of NS IP Address

XenServer

Aug 18, 2015

The entities on which you can perform NetScaler SDX CLI operations:

- appliance - Xen
- channel - Channels on the system
- channelinfo - Provides platfor specific channel information
- cleaninstall - Xen Upgrade
- cpucoreusage - Host CPU Cores
- hostinterface - XenServer Interface
- raidLogicalDrive - Raid Logical Drive
- raidPhysicalDrive - Raid Physical Drive
- systemhealth - Health Summary
- systemhealthHardware - Hardware Resource
- systemhealthSoftware - Software Resource
- systemhealthStorageRepository - Storage Repository
- systemhealthdisk - Disk IO Statistics
- systemhealthfanspeed - Xen Health Monitor (IPMI Sensor) - Fan Speed
- systemhealthpowersupply - Xen Health Monitor (IPMI Sensor) - Miscellaneous
- systemhealthtemperature - Xen Health Monitor (IPMI Sensor) - Temperature
- systemhealthvoltage - Xen Health Monitor (IPMI Sensor) - Voltage
- xenhotfix - Xen Hotfix
- xennsvpximage - NetScaler XVA File
- xensupplementalpack - XenServer Supplemental Pack
- xenupgrade - Xen Upgrade

appliance

Aug 18, 2015
Xen

do stop | show | do reboot

do appliance stop

Use this operation to shutdown XenServer

Synopsys

do appliance stop [id=<string>]

Parameters

id

Id is system generated key for all the XenServers

---

show appliance

Use this operation to get XenServers

Synopsys

show appliance [id=<string>]

Parameters

id

Id is system generated key for all the XenServers

---

do appliance reboot

Use this operation to reboot XenServer

Synopsys

do appliance reboot [id=<string>]

Parameters

id

Id is system generated key for all the XenServers

---

channel

Aug 18, 2015

Channels on the system

show | delete | set | add

show channel

Use this operation to get channel

Synopsys

show channel

---

delete channel

Use this operation to delete channels

Synopsys

delete channel channel_id=<string> [mtu=<int>] [static_channel_state=(false | true)] [channel_alias=<string>] [state=<string>] [channel_tag_all_vlans=(false | true)] [channel_type=<string>] [lacp_channel_time=<string>] [channel_bandwidth_high=<int>] [channel_ha_monitoring=(false | true)] [channel_throughput=<int>] [channel_bandwidth_normal=<int>] [channel_interface_list=<string...>]

Parameters

channel_id

Channel ID if this interface represents a channel (LA/1, LA/2 ...)

This is a mandatory parameter.

mtu

MTU value, should be between 1500-9126

static_channel_state

Static channel state (Enabled/Disabled)

channel_alias

Alias name for this channel

state

State of the port.

channel_tag_all_vlans

If true then all the member interfaces of this channel are tagged. Possible values: true and false

channel_type

Channel type if this interface represents a channel (LACP or Static)

lacp_channel_time

LACP time. Possible values: SHORT and LONG

channel_bandwidth_high

Higher end threshold of the channel bandwidth usage in Mbps

channel_ha_monitoring

HA-monitoring control for the channel. Possible values: true and false

channel_throughput

Minimum required throughput in Mbps for this channel

channel_bandwidth_normal

Lower end threshold of the channel bandwidth usage in Mbps

channel_interface_list

Comma separated list of interfaces that are part of this channel if this interface represents a channel (10/1, 10/4)

---

set channel

Use this operation to modify channel

Synopsys

set channel channel_id=<string> [mtu=<int>] [static_channel_state=(false | true)] [channel_alias=<string>] [state=<string>] [channel_tag_all_vlans=(false | true)] [channel_type=<string>] [lacp_channel_time=<string>] [channel_bandwidth_high=<int>] [channel_ha_monitoring=(false | true)] [channel_throughput=<int>] [channel_bandwidth_normal=<int>] [channel_interface_list=<string...>]

Parameters

channel_id

Channel ID if this interface represents a channel (LA/1, LA/2 ...)

This is a mandatory parameter.

mtu

MTU value, should be between 1500-9126

static_channel_state

Static channel state (Enabled/Disabled)

channel_alias

Alias name for this channel

state

State of the port.

channel_tag_all_vlans

If true then all the member interfaces of this channel are tagged. Possible values: true and false

channel_type

Channel type if this interface represents a channel (LACP or Static)

lacp_channel_time

LACP time. Possible values: SHORT and LONG

channel_bandwidth_high

Higher end threshold of the channel bandwidth usage in Mbps

channel_ha_monitoring

HA-monitoring control for the channel. Possible values: true and false

channel_throughput

Minimum required throughput in Mbps for this channel

channel_bandwidth_normal

Lower end threshold of the channel bandwidth usage in Mbps

channel_interface_list

Comma separated list of interfaces that are part of this channel if this interface represents a channel (10/1, 10/4)

---

add channel

Use this operation to create channel

Synopsys

add channel static_channel_state=(false | true) channel_id=<string> channel_type=<string> channel_interface_list=<string...> [mtu=<int>] [channel_alias=<string>] [state=<string>] [channel_tag_all_vlans=(false | true)] [lacp_channel_time=<string>] [channel_bandwidth_high=<int>] [channel_ha_monitoring=(false | true)] [channel_throughput=<int>] [channel_bandwidth_normal=<int>]

Parameters

static_channel_state

Static channel state (Enabled/Disabled)

This is a mandatory parameter.

channel_id

Channel ID if this interface represents a channel (LA/1, LA/2 ...)

This is a mandatory parameter.

channel_type

Channel type if this interface represents a channel (LACP or Static)

This is a mandatory parameter.

channel_interface_list

Comma separated list of interfaces that are part of this channel if this interface represents a channel (10/1, 10/4)

This is a mandatory parameter.

mtu

MTU value, should be between 1500-9126

channel_alias

Alias name for this channel

state

State of the port.

channel_tag_all_vlans

If true then all the member interfaces of this channel are tagged. Possible values: true and false

lacp_channel_time

LACP time. Possible values: SHORT and LONG

channel_bandwidth_high

Higher end threshold of the channel bandwidth usage in Mbps

channel_ha_monitoring

HA-monitoring control for the channel. Possible values: true and false

channel_throughput

Minimum required throughput in Mbps for this channel

channel_bandwidth_normal

Lower end threshold of the channel bandwidth usage in Mbps

channelinfo

Aug 18, 2015

Provides platfor specific channel information

show channelinfo

Use this operation to get channelinfo

Synopsys

show channelinfo

cleaninstall

Aug 18, 2015
Xen Upgrade

show | add

show cleaninstall

Use this operation to findout if clean-install is supported or not

Synopsys

show cleaninstall

---

add cleaninstall

Use this operation to start the clean-install

Synopsys

add cleaninstall image_name=<string> [is_supported=(false | true)]

Parameters

image_name

image_name

This is a mandatory parameter.

is_supported

Is Clean-Install supported

---

cpucoreusage

Aug 18, 2015

Host CPU Cores

show cpucoreusage

Use this operation to get CPU Cores

Synopsys

show cpucoreusage

hostinterface

Aug 18, 2015

XenServer Interface

show | set | do custom

show hostinterface

Use this operation to get interface/channel

Synopsys

show hostinterface [id=<string>]

Parameters

id

Id is system generated key

---

set hostinterface

Use this operation to modify interface/channel

Synopsys

set hostinterface mapped_port=<string> [mtu=<int>] [port=<string>] [apply_mac_address=(false | true)] [range=<string>] [base_mac_address=<string>] [add_mac_address=(false | true)] [interface_type=<string>] [flow_control_tx=(false | true)] [adv_auto_neg=(false | true)] [speed=<string>] [cpu_socket=<string>] [flow_control_rx=(false | true)] [state=<string>] [flow_control_auto_neg=(false | true)] [act_id=<string>] [device_name=<string>] [port_type=<string>] [duplex=<string>]

Parameters

mapped_port

Mapped Port Name Ex: eth0

This is a mandatory parameter.

mtu

MTU value, should be between 1500-9126

port

Port Name Ex: 10/1

apply_mac_address

Apply Mac Address

range

Range for Base Mac Address

base_mac_address

Mac Address

add_mac_address

Add Mac Address

interface_type

Indicates if this is an interface or a channel or a member interface of a channel

flow_control_tx

TX Pause

adv_auto_neg

true if the advertised auto-negotiation for the port is true

speed

Actual speed

cpu_socket

CPU Socket to which this interface belong to

flow_control_rx

RX Pause

state

State of the port.

flow_control_auto_neg

Auto Negotiation For Flow Control

act_id

Activity Id

device_name

Device Name

port_type

Port Type

duplex

Duplex

---

do hostinterface custom

Use this operation to reset interface settings

Synopsys

do hostinterface custom [id=<string>]

Parameters

id

Id is system generated key

---

raidLogicalDrive

Aug 18, 2015

Raid Logical Drive

show | delete | add

show raidLogicalDrive

Use this operation to get logical disks

Synopsys

show raidLogicalDrive [id=<string>]

Parameters

id

Id is system generated key for all logical drives

---

delete raidLogicalDrive

Use this operation to delete logical disk

Synopsys

delete raidLogicalDrive [id=<string>]

Parameters

id

Id is system generated key for all logical drives

---

add raidLogicalDrive

Use this operation to create logical disk

Synopsys

add raidLogicalDrive [name=<string>] [adapter_id=<int>] [state=<string>] [drives=<string>] [targetid=<int>] [virtualdrive=<int>] [size=<string>] [physical_disk_slot_1=<string>] [physical_disk_slot_2=<string>]

Parameters

name

Logical Drive Name

adapter_id

Adapter ID

state

State

drives

Drives

targetid

Target ID

virtualdrive

Virtual Drive

size

Logical Drive Size

physical_disk_slot_1

First Slot for Raid Logical Drive

physical_disk_slot_2

Second Slot for Raid Logical Drive

raidPhysicalDrive

Aug 18, 2015

Raid Physical Drive

do make_good_pd | show | do remove_pd | do locate_pd_start | do locate_pd_stop | do replace_missing

do raidPhysicalDrive make_good_pd

Use this operation to make good physical disks

Synopsys

do raidPhysicalDrive make_good_pd [slot=<int>]

Parameters

slot

Slot Number

---

show raidPhysicalDrive

Use this operation to get physical disks

Synopsys

show raidPhysicalDrive [slot=<int>]

Parameters

slot

Slot Number

---

do raidPhysicalDrive remove_pd

Use this operation to remove physical disks

Synopsys

do raidPhysicalDrive remove_pd [slot=<int>]

Parameters

slot

Slot Number

---

do raidPhysicalDrive locate_pd_start

Use this operation to locate physical disks

Synopsys

do raidPhysicalDrive locate_pd_start [slot=<int>]

Parameters

slot

Slot Number

---

do raidPhysicalDrive locate_pd_stop

Use this operation to stop locating physical disks

Synopsys

do raidPhysicalDrive locate_pd_stop [slot=<int>]

Parameters

slot

Slot Number

---

do raidPhysicalDrive replace_missing

Use this operation to replace missing physical disks

Synopsys

do raidPhysicalDrive replace_missing [slot=<int>]

Parameters

slot

Slot Number

---

systemhealth

Aug 18, 2015

Health Summary

show systemhealth

Use this operation to get health of the SDX system resource

Synopsys

show systemhealth [id=<string>]

Parameters

id

Id is system generated key

systemhealthHardware

Aug 18, 2015

Hardware Resource

show systemhealthHardware

Use this operation to get the current values of hardware resources

Synopsys

show systemhealthHardware

systemhealthSoftware

Aug 18, 2015

Software Resource

show systemhealthSoftware

Use this operation to get the current values of software resources

Synopsys

show systemhealthSoftware

systemhealthStorageRepository

Aug 18, 2015

Storage Repository

show systemhealthStorageRepository

Use this operation to get details of the storage repositories

Synopsys

show systemhealthStorageRepository [bay_number=<string>]

Parameters

bay_number

Bay number

systemhealthdisk

Aug 18, 2015

Disk IO Statistics

show systemhealthdisk

Use this operation to get disk IO statistics

Synopsys

show systemhealthdisk [name=<string>]

Parameters

name

Name of the Disk

systemhealthfanspeed

Aug 18, 2015

Xen Health Monitor (IPMI Sensor) - Fan Speed

show systemhealthfanspeed

Use this operation to get the IPMI sensor data (for all fan-speed sensors)

Synopsys

show systemhealthfanspeed

systemhealthpowersupply

Aug 18, 2015

Xen Health Monitor (IPMI Sensor) - Miscellaneous

show systemhealthpowersupply

Use this operation to get the IPMI Sensor data (for all miscellaneous sensors)

Synopsys

show systemhealthpowersupply

systemhealthtemperature

Aug 18, 2015

Xen Health Monitor (IPMI Sensor) - Temperature

show systemhealthtemperature

Use this operation to get the IPMI sensor data (for all temperature sensors)

Synopsys

show systemhealthtemperature

systemhealthvoltage

Aug 18, 2015

Xen Health Monitor (IPMI Sensor) - Voltage

show systemhealthvoltage

Use this operation to get the IPMI sensor data (for all voltage sensors)

Synopsys

show systemhealthvoltage

xenhotfix

Aug 18, 2015
Xen Hotfix

show | delete | do custom

show xenhotfix

Use this operation to get xen hotfix

Synopsys

show xenhotfix [file_name=<string>]

Parameters

file_name

File Name

---

delete xenhotfix

Use this operation to delete xen hotfix

Synopsys

delete xenhotfix file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

do xenhotfix custom

Use this operation to apply new xen hotfixes

Synopsys

do xenhotfix custom [file_name=<string>]

Parameters

file_name

File Name

xennsvpximage

Aug 18, 2015

NetScaler XVA File

show | delete

show xennsvpximage

Use this operation to get NetScaler XVA file

Synopsys

show xennsvpximage [file_name=<string>]

Parameters

file_name

File Name

---

delete xennsvpximage

Use this operation to delete NetScaler XVA file

Synopsys

delete xennsvpximage file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

xensupplementalpack

Aug 18, 2015

XenServer Supplemental Pack

show | delete | do custom

show xensupplementalpack

Use this operation to get xen supplemental packs

Synopsys

show xensupplementalpack [file_name=<string>]

Parameters

file_name

File Name

---

delete xensupplementalpack

Use this operation to delete xen supplemental pack

Synopsys

delete xensupplementalpack file_name=<string>

Parameters

file_name

File Name

This is a mandatory parameter.

---

do xensupplementalpack custom

Use this operation to install new xen supplemental pack

Synopsys

do xensupplementalpack custom [file_name=<string>]

Parameters

file_name

File Name

xenupgrade

Aug 18, 2015

Xen Upgrade

do xenupgrade custom

Use this operation to upgrade XenServer

Synopsys

do xenupgrade custom [image_name=<string>]

Parameters

image_name

image_name