Configuring the External Authentication Server 86
Configuring Link Aggregation from the Management Service 91
Configuring a Channel from the Management Service 92
Set up a cluster of Citrix ADC instances 93
Configuring SSL Ciphers to Securely Access the Management Service 95
Backing Up and Restoring the Configuration Data of the SDX Appliance 104
Performing Appliance Reset 108
Cascading External Authentication Servers 111
Provisioning Citrix NetScaler instances 112
Provisioning Third-Party Virtual Machines 128
SECUREMATRIX GSB 129
Trend Micro InterScan Web Security 133
Websense Protector 134
BlueCat DNS/DHCP 138
CA Access Gateway 141
Palo Alto Networks VM-Series 143
Manage crypto capacity 146
Bandwidth Metering in SDX 152
Configuring and Managing Citrix NetScaler instances 155
Monitoring Citrix NetScaler instances 158
Using Logs to Monitor Operations and Events 162
Use Cases for Citrix ADC SDX Appliances 165
Consolidation When the Management Service and the Citrix ADC instances are in the Same Network 165

© 1999-2020 Citrix Systems, Inc. All rights reserved.
Consolidation When the Management Service and the Citrix NetScaler instances are in Different Networks

Consolidation Across Security Zones

Consolidation with Dedicated Interfaces for Each Instance

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

NITRO API

Obtaining the NITRO package

.NET SDK

REST Web Services

How NITRO works

Java SDK

SDX Command Reference
NetScaler SDX 11.1

Introduction

January 23, 2019

The Citrix NetScaler SDX appliance is a multitenant platform on which you can provision and manage multiple Citrix NetScaler virtual 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 SDX appliance provides a Management Service that is preprovisioned 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.

For information different SDX hardware platforms and how to set up the SDX hardware, see the SDX hardware documentation: Citrix ADC SDX

Release Notes

August 16, 2018

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

For detailed information about SDX 11.1 enhancements, known issues, and bug fixes, see NetScaler Release Notes.
Getting started with the Management Service user interface

January 23, 2019

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

Logging on to the Management Service user interface

To log on to the Management Service user interface

1. In your Web browser address field, type one of the following:
   
   http://Management Service IP Address
   or
   https://Management Service IP Address

2. On the Login page, in User Name and Password, type the user name and password of the Management Service. The default user name and password are nsroot and nsroot. However, Citrix recommends that you change the password after initial configuration. For information about changing the nsroot password, see Changing the Password of the Default User Account.

3. Click Show Options, and then do the following:

   a) In the Start in list, select the page that must be displayed immediately after you log on to the user interface. The available options are Home, Monitoring, Configuration, Documentation, and Downloads. For example, if you want the Management Service to display the Configuration page when you log on, select Configuration in the Start in list.

   b) In Timeout, type the length of time (in minutes, hours, or days) after which you want the session to expire. The minimum timeout value is 15 minutes.

   The Start in and Timeout settings persist across sessions. Their default values are restored only after you clear the cache.

4. Click Login to log on to the Management Service user interface.
**Initial Setup Wizard**

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

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

You can also use this wizard to modify the network configuration details that you specified for the 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 IPAddress**—IP address of the XenServer server.
- **Management Service IPAddress**—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 Citrix 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 to 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.

**Provision instances on an SDX appliance**

You can provision one or more NetScaler or third-party instances on the SDX appliance by using the Management Service. The number of instances that you can install depends on the license you have purchased. If the number of instances added is equal to the number specified in the license, the Management Service does not allow provisioning more instances.
For information about provisioning third-party instances, see Provisioning Third-Party Virtual Machines.

**Console access**

You can access the console of Citrix 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 SDX appliance.

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

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

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

**Management Service Statistics**

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

![Management Service Statistics](image)

**Single Sign-On to the Management Service and the Citrix NetScaler instances**

Logging on to the Management Service gives you direct access to the Citrix 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.
Managing the home page

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

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

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

- **System CPU and 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.

- **Citrix NetScaler instances**
  Displays the properties of the Citrix 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 Citrix 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 Citrix NetScaler instance details**
  You can view and hide the details of a particular Citrix 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.

### Ports

The following ports must be open on the SDX appliance for it to function properly.

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>80</td>
<td>Used for incoming HTTP (GUI and NITRO) requests. One of the primary interfaces to access the SDX Management Service interface.</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>Used for incoming secured HTTP (GUI and NITRO) requests. One of the primary interfaces to access the SDX Management Service interface.</td>
</tr>
<tr>
<td>TCP</td>
<td>22</td>
<td>Used for SSH and SCP access to the SDX Management Service interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Port</td>
<td>Details</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>UDP</td>
<td>162</td>
<td>The SDX Management Service interface listens for SNMP traps from the Citrix NetScaler instances hosted on the SDX appliance.</td>
</tr>
<tr>
<td>UDP</td>
<td>161</td>
<td>The SDX Management Service interface listens for SNMP walks/get requests.</td>
</tr>
</tbody>
</table>

**Single bundle upgrade**

January 23, 2019

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

The Single bundle upgrade, available from 11.0 and later releases, combines all the components except the Citrix NetScaler VPX instance image and LOM firmware in a single image file, called the SDX image. Using this 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 is always running a version that is tested and supported by Citrix. Because all the SDX components are combined in a single file, the SDX image file is significantly larger than the Management Service image file.

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

**Points to note**

- 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.

Upgrading the entire appliance to 11.1

If you are currently running version 10.5.66.x or later of the SDX Management Service, you can use the SDX 11.1 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. Go to step 3. If you’re upgrading from release 10.55 66.x and later. Go to step 4, if you’re upgrading from release 11.0
3. In the System Administration group, click Upgrade Management Service.
4. In the System Administration group, click Upgrade Appliance.

The upgrade process takes a few minutes.

Before the upgrade, Management Service displays the following information:

• Single bundle image file name
• The current version of SDX running on your appliance
• The selected version to which the appliance will be 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.

Related information

Demystifying the NetScaler SDX appliance upgrade process
Upgrading a Citrix NetScaler instance

January 23, 2019

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

You have to upload the Citrix NetScaler software images to the Citrix NetScaler SDX appliance before upgrading the Citrix NetScaler instances. For installing a new instance, you need the Citrix NetScaler XVA file.

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

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

- **Last Modified**
  Date when the file was last modified.

- **Size**
  Size, in MB, of the file.

**To Upload a Software Image**

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

**To Create a Backup by Downloading a Build File**

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

**To Upload a XVA File**

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

**To Create a Backup by Downloading an XVA File**

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

**Upgrading Citrix NetScaler VPX Instances**

You can use the Management Service to upgrade one or more of the 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 Citrix NetScaler instance and want to upgrade the instance from Citrix NetScaler release 10 to release 10.1 or later, you must delete all the channels from the Citrix NetScaler instance, upgrade the instance, and then create LACP channels from the Management Service. If you are downgrading the Citrix NetScaler instance from release 10.1 to 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 VPX instance.

- **Important**

Use the SDX Management Service only and not the VPX GUI to upgrade 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 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.

Related information

Demystifying the NetScaler SDX appliance upgrade process

Manage and monitor the SDX appliance

January 23, 2019

After your Citrix NetScaler 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.

Modify the network configuration of the SDX appliance

You can modify the network configuration details that you provided for the 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.

Change the password of the default user account

The default user account provides complete access to all features of the Citrix 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 pass-
word 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.

**Modify 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**.

**Modify the hostname of the appliance**

You can change the hostname of the Management Service.

**VLAN filtering**

VLAN filtering provides segregation of data between VPX instances that share a physical port. For example, if you have configured two 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 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 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 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.
NetScaler SDX 11.1

Configure clock synchronization

You can configure your 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 Citrix 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 ADC 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.

To enable NTP synchronization

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

To modify authentication options

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

**View 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 GUI click **Dashboard** and check **System Throughput (Mbps)**.

**View real-time CPU and memory usage**

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

To view the CPU and memory usage of the SDX appliance, on the GUI click **Dashboard** and check **Management Service Statistics**.

**View CPU usage for all cores**

You can view the usage of each CPU core on the 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 GUI click **Dashboard** and check **System CPU Usage (%)**.

**Install an SSL certificate on the SDX appliance**

The 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.

**View the SSL certificate on the Management Service**

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

To view the SSL certificate, click System and in the Set Up Appliance group, click **View SSL Certificate**.

**SSL certificates and keys for Citrix NetScaler instances**

Separate views of SSL certificates and keys for Citrix 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 Citrix NetScaler instances.

To access the SSL certificates and keys for Citrix NetScaler instances, navigate to **Configuration > NetScaler > SSL Certificate Files**.
Modify system settings

For security reasons, you can specify that the Management Service and a 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 to 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**.

Restart the appliance

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

To restart the appliance, click **Configuration > System** and in the System Administration group, click **Reboot Appliance**.

Shut down the appliance

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

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

Create SDX administrative domains

January 23, 2019
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 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 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>
<thead>
<tr>
<th>Table 1. Owner Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU core</strong></td>
</tr>
<tr>
<td><strong>Throughput (Mbps)</strong></td>
</tr>
<tr>
<td><strong>Memory (MB)</strong></td>
</tr>
<tr>
<td><strong>Disk Space (GB)</strong></td>
</tr>
<tr>
<td><strong>SSL Chips</strong></td>
</tr>
<tr>
<td><strong>Instances</strong></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Resource</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU core</td>
<td>5</td>
</tr>
<tr>
<td>Throughput (Mbps)</td>
<td>1024</td>
</tr>
<tr>
<td>Memory (MB)</td>
<td>2048</td>
</tr>
<tr>
<td>Disk Space (GB)</td>
<td>40</td>
</tr>
<tr>
<td>SSL Chips</td>
<td>8</td>
</tr>
<tr>
<td>Instances</td>
<td>4</td>
</tr>
</tbody>
</table>

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.

**Assign 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.

**Manage RAID disk allocation on 22XXX SDX appliances**

January 23, 2019

Citrix 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 SDX appliance, because the appliance hosts a large number of virtual machines, and a disk failure...
NetScaler SDX 1.1

affects multiple virtual machines. The RAID controller on the Management Service supports the RAID 1 configuration, which implements disk mirroring. That is, two disks maintain the same data. If a disk in the RAID 1 array fails, its mirror immediately supplies all needed data.

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

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

View drive properties and operations

A 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.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimal</td>
<td>The virtual drive operating condition is good.</td>
</tr>
<tr>
<td></td>
<td>All configured drives are online.</td>
</tr>
<tr>
<td>Degraded</td>
<td>The virtual drive operating condition is not optimal.</td>
</tr>
<tr>
<td></td>
<td>One of the configured drives has failed or is offline.</td>
</tr>
<tr>
<td>Failed</td>
<td>The virtual drive has failed.</td>
</tr>
<tr>
<td>Offline</td>
<td>The virtual drive is not available to the RAID controller.</td>
</tr>
</tbody>
</table>
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 SDX appliance supports a maximum of eight physical slots, that is, a pair of four slots on each side of the appliance. On the **Configuration > System > RAID > Physical Drives** tab, you can view the following information:

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

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

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

On the Configuration > System > RAID > **Storage Repository** tab, you can view the status of storage repositories on 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.

**Add 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:
   a) In the **First Slot** drop-down list, select 4.
   b) In the **Second Slot** drop-down list, select 5.
   c) 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.

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

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

**SDX licensing overview**

January 23, 2019

In the Citrix 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.”

**Prerequisites**

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.
Allocate your license by using the Management Service

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 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**.

![Hardware Serial Number Dialog](image)

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.
**SDX Resource Visualizer**

January 23, 2019

When a Citrix NetScaler instance is provisioned on a Citrix NetScaler SDX appliance, various resources such as CPU, throughput, memory need to be allocated to an instance. With current 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

June 18, 2019

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 SDX appliance, and assign MAC addresses to interfaces.

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

In the list of Interfaces in the Interfaces pane, in the State column, UP indicates that the interface is receiving traffic normally. DOWN indicates a network issue because of which the interface is unable to send or receive traffic.

To configure an interface

1. On the Configuration tab, in the navigation pane, expand System, and then click Interfaces.
2. In the Interfaces pane, click the interface that you want to configure, and then click Edit.
3. In the Configure Interface window, specify values for the following parameters:
   - Auto Negotiation* — Enable auto-negotiation. Possible values: ON, OFF. Default: ON.
   - 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* — Enable Tx flow control is enabled. Possible values: ON, OFF. Default: ON

   * A required parameter

4. Click OK, and then click Close.

To reset the parameters of an interface to their default values

1. On the Configuration tab, in the navigation pane, expand System, and then click Interfaces.
2. In the Interfaces pane, click the interface that you want to reset, and then click Reset.
Display the mapping of virtual interfaces on the VPX instance to the physical interfaces on the SDX appliance

If you log on to the Citrix NetScaler VPX 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 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 CLI, 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(28799153) 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.
```

Assigning a MAC Address to an Interface

If, while you are provisioning a Citrix 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

<table>
<thead>
<tr>
<th>Physical interface</th>
<th>Base MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>00:00:00:00:00:00</td>
</tr>
<tr>
<td>0/2</td>
<td>00:00:00:00:00:08</td>
</tr>
<tr>
<td>1/1</td>
<td>00:00:00:00:00:10</td>
</tr>
<tr>
<td>1/2</td>
<td>00:00:00:00:00:18</td>
</tr>
<tr>
<td>1/3</td>
<td>00:00:00:00:00:20</td>
</tr>
<tr>
<td>1/4</td>
<td>00:00:00:00:00:28</td>
</tr>
<tr>
<td>1/5</td>
<td>00:00:00:00:00:30</td>
</tr>
<tr>
<td>1/6</td>
<td>00:00:00:00:00:38</td>
</tr>
<tr>
<td>1/7</td>
<td>00:00:00:00:00:40</td>
</tr>
<tr>
<td>1/8</td>
<td>00:00:00:00:00:48</td>
</tr>
<tr>
<td>10/1</td>
<td>00:00:00:00:00:50</td>
</tr>
<tr>
<td>10/2</td>
<td>00:00:00:00:00:90</td>
</tr>
</tbody>
</table>

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 the Configure Interface window.

**Disable or enable the physical interfaces on the SDX appliance**

If you are not using any of the physical interfaces on the SDX appliance, for security purpose, you can disable the physical interface using the Management Service.

Note: By default, all the physical interfaces on the SDX appliance is enabled. Also, if an interface is used by an VPX or channel, you cannot disable the interface.

**To disable the physical interface:**

1. On the **Configuration** tab, in the navigation pane, expand **System**, and then click **Interfaces**.
2. In the **Interfaces** pane, select the interface that you want to disable.
3. In the **Action** drop-down list, click **Disable**.

© 1999-2020 Citrix Systems, Inc. All rights reserved.
If you want to use the disabled physical interface, you can enable the interface using the Management Service.

To enable the disabled physical interface:

1. On the Configuration tab, in the navigation pane, expand System, and then click Interfaces.
2. In the Interfaces pane, select the disable interface that you want to enable.
3. In the Action drop-down list, click Enable.

**Jumbo frames on SDX appliances**

January 23, 2019

Citrix 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 Citrix NetScaler SDX 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 Citrix NetScaler instances provisioned on 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.

**Use case: Jumbo-to-jumbo setup**

Consider an example of a jumbo to jumbo setup in which SIP load balancing virtual server LBVS-1, configured on Citrix 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.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of client CL1</td>
<td>CL1</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>IP address of servers</td>
<td>S1</td>
<td>198.51.100.19</td>
</tr>
<tr>
<td></td>
<td>S2</td>
<td>198.51.100.20</td>
</tr>
<tr>
<td>MTUs specified for interfaces</td>
<td>10/1</td>
<td>9000</td>
</tr>
<tr>
<td>(by using the Management Service interface)</td>
<td>10/2</td>
<td>9000</td>
</tr>
<tr>
<td>and VLANs on NS1 (by using the CLI).</td>
<td>VLAN 10</td>
<td>9000</td>
</tr>
<tr>
<td></td>
<td>VLAN 20</td>
<td>9000</td>
</tr>
<tr>
<td>Services on NS1 representing servers</td>
<td>SVC-S1</td>
<td>IP address: 198.51.100.19;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol: SIP;Port: 5060</td>
</tr>
<tr>
<td>Services on NS1 representing servers</td>
<td>SVC-S2</td>
<td>IP address: 198.51.100.20;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol: SIP;Port: 5060</td>
</tr>
</tbody>
</table>
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 and third 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 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 Citrix 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 Citrix NetScaler instances.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>NetScaler Command Syntax</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create VLANS and set the MTU of the desired VLANS for supporting jumbo frames.</td>
<td>add vlan &lt;id&gt; -mtu &lt;positive_integer&gt; show vlan &lt;id&gt;</td>
<td>add vlan 10 -mtu 9000; add vlan 20 -mtu 9000</td>
</tr>
<tr>
<td>Bind interfaces to VLANS.</td>
<td>bind vlan &lt;id&gt; -ifnum &lt;interface_name&gt;; show vlan &lt;id&gt;</td>
<td>bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2</td>
</tr>
<tr>
<td>Add a SNIP address.</td>
<td>add ns ip &lt;IPAddress&gt; &lt;netmask&gt; -type SNIP; show ns ip</td>
<td>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</td>
</tr>
<tr>
<td>Create services representing SIP servers.</td>
<td>add service &lt;serviceName&gt; &lt;ip&gt; SIP_UDP &lt;port&gt;; show service &lt;name&gt;</td>
<td>add service SVC-S1 198.51.100.19 SIP_UDP 5060; dd service SVC-S2 198.51.100.20 SIP_UDP 5060</td>
</tr>
</tbody>
</table>
Use Case: Non-Jumbo to Jumbo Setup

Consider an example of a non-jumbo to jumbo setup in which load balancing virtual server LBVS1, configured on a Citrix 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.

© 1999-2020 Citrix Systems, Inc. All rights reserved.
The following table lists the settings used in this example:

<table>
<thead>
<tr>
<th>Entity</th>
<th>Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of client CL1</td>
<td>CL1</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td>IP address of servers</td>
<td>S1</td>
<td>198.51.100.19</td>
</tr>
<tr>
<td></td>
<td>S2</td>
<td>198.51.100.20</td>
</tr>
<tr>
<td>MTU for interface 10/1 (by using the Management Service interface).</td>
<td></td>
<td>1500</td>
</tr>
<tr>
<td>MTU set for interface 10/2 (by using the Management Service interface).</td>
<td></td>
<td>9000</td>
</tr>
<tr>
<td>MTU for VLAN 10 on NS1 (by using NetScaler command line interface).</td>
<td></td>
<td>1500</td>
</tr>
<tr>
<td>MTU set for VLAN 20 on NS1 (by using NetScaler command line interface).</td>
<td></td>
<td>9000</td>
</tr>
<tr>
<td>Services on NS1 representing servers</td>
<td>SVC-S1</td>
<td>IP address: 198.51.100.19; Protocol: HTTP; Port: 80; MSS: 8960</td>
</tr>
<tr>
<td>Entity</td>
<td>Name</td>
<td>Details</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>SVC-S2</td>
<td>IP address: 198.51.100.20; Protocol: HTTP; Port: 80; MSS: 8960</td>
</tr>
<tr>
<td>Load balancing virtual server on VLAN 10</td>
<td>LBVS-1</td>
<td>IP address: 203.0.113.15; Protocol: HTTP; Port: 80; Bound services: SVC-S1, SVC-S2; MSS: 1460</td>
</tr>
</tbody>
</table>

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.
   a) Size of the request packet = \[\text{IP Header} + \text{TCP Header} + \text{TCP Request}\] = \[20 + 20 + 200\] = 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.
   a) Size of the request packet = \[\text{IP Header} + \text{TCP Header} + \text{TCP Request}\] = \[20 + 20 + 200\] = 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 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 Citrix 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 Citrix NetScaler instances.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>NetScaler Command Line Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create VLANs and set the MTU of the desired VLANs for supporting jumbo frames.</td>
<td>add vlan &lt;id&gt; -mtu &lt;positive_integer&gt;; show vlan &lt;id&gt;</td>
<td>add vlan 10 -mtu 1500; add vlan 20 -mtu 9000</td>
</tr>
<tr>
<td>Bind interfaces to VLANs.</td>
<td>bind vlan &lt;id&gt; -ifnum &lt;interface_name&gt;; show vlan &lt;id&gt;</td>
<td>bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2</td>
</tr>
</tbody>
</table>
NetScaler SDX 11.1

<table>
<thead>
<tr>
<th>Tasks</th>
<th>NetScaler Command Line Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add a SNIP address.</strong></td>
<td>add ns ip &lt;IPAddress&gt; &lt;netmask&gt; -type SNIP; show ns ip</td>
<td>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</td>
</tr>
<tr>
<td><strong>Create services representing HTTP servers</strong></td>
<td>add service &lt;serviceName&gt; &lt;ip&gt; HTTP &lt;port&gt;; show service &lt;name&gt;</td>
<td>add service SVC-S1 198.51.100.19 http 80; add service SVC-S2 198.51.100.20 http 80</td>
</tr>
<tr>
<td><strong>Create HTTP load balancing virtual servers and bind the services to it</strong></td>
<td>add lb vserver &lt;name&gt; HTTP &lt;ip&gt; &lt;port&gt;; bind lb vserver &lt;vserverName&gt; &lt;serviceName&gt;; show lb vserver &lt;name&gt;</td>
<td>add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1</td>
</tr>
<tr>
<td><strong>Create a custom TCP profile and set its MSS for supporting jumbo frames.</strong></td>
<td>add tcpProfile &lt;name&gt; -mss &lt;positive_integer&gt;; show tcpProfile &lt;name&gt;</td>
<td>add tcpProfile NS1-SERVERS-JUMBO -mss 8960</td>
</tr>
<tr>
<td><strong>Bind the custom TCP profile to the desired services.</strong></td>
<td>set service &lt;Name&gt; -tcpProfileName &lt;string&gt;; show service &lt;name&gt;</td>
<td>set service SVC-S1 -tcpProfileName NS1-SERVERS-JUMBO; set service SVC-S2 -tcpProfileName NS1-SERVERS-JUMBO</td>
</tr>
<tr>
<td><strong>Save the configuration</strong></td>
<td>save ns config; show ns config</td>
<td></td>
</tr>
</tbody>
</table>

**Use case: Coexistence of jumbo and non-jumbo flows on same set of interfaces**

Consider an example in which load balancing virtual servers LBVS1 and LBVS2 are configured on Citrix 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.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of clients</td>
<td>CL1</td>
<td>192.0.2.10</td>
</tr>
<tr>
<td></td>
<td>CL2</td>
<td>192.0.2.20</td>
</tr>
<tr>
<td>IP address of servers</td>
<td>S1</td>
<td>198.51.100.19</td>
</tr>
<tr>
<td></td>
<td>S2</td>
<td>198.51.100.20</td>
</tr>
<tr>
<td></td>
<td>S3</td>
<td>198.51.101.19</td>
</tr>
<tr>
<td></td>
<td>S4</td>
<td>198.51.101.20</td>
</tr>
<tr>
<td>SNIP addresses on NS1</td>
<td></td>
<td>198.51.100.18; 198.51.101.18</td>
</tr>
<tr>
<td>MTU specified for interfaces</td>
<td>10/1</td>
<td>9216</td>
</tr>
<tr>
<td>and VLANs on NS1</td>
<td>10/2</td>
<td>9216</td>
</tr>
<tr>
<td>VLAN 10</td>
<td></td>
<td>9000</td>
</tr>
<tr>
<td>VLAN 20</td>
<td></td>
<td>9000</td>
</tr>
<tr>
<td>VLAN 30</td>
<td></td>
<td>9000</td>
</tr>
<tr>
<td>VLAN 40</td>
<td></td>
<td>1500</td>
</tr>
<tr>
<td>Default TCP profile</td>
<td>nstcp_default_profile</td>
<td>MSS: 1460</td>
</tr>
<tr>
<td>Custom TCP profile</td>
<td>ALL-JUMBO</td>
<td>MSS: 8960</td>
</tr>
<tr>
<td>Services on NS1 representing servers</td>
<td>SVC-S1</td>
<td>IP address: 198.51.100.19; Protocol: HTTP; Port: 80; TCP profile: ALL-JUMBO (MSS: 8960)</td>
</tr>
<tr>
<td></td>
<td>SVC-S2</td>
<td>IP address: 198.51.100.20; Protocol: HTTP; Port: 80; TCP profile: ALL-JUMBO (MSS: 8960)</td>
</tr>
<tr>
<td></td>
<td>SVC-S3</td>
<td>IP address: 198.51.101.19; Protocol: HTTP; Port: 80; TCP profile: nstcp_default_profile (MSS:1460)</td>
</tr>
</tbody>
</table>
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 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 Citrix 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 Citrix NetScaler instances.
<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create VLANs and set the MTU of the desired VLANs for supporting jumbo frames.</td>
<td>add vlan &lt;id&gt; -mtu &lt;positive_integer&gt;; show vlan &lt;id&gt;</td>
<td>add vlan 10 -mtu 9000; add vlan 20 -mtu 9000; add vlan 30 -mtu 1500; add vlan 40 -mtu 1500</td>
</tr>
<tr>
<td>Bind interfaces to VLANs.</td>
<td>bind vlan &lt;id&gt; -ifnum &lt;interface_name&gt;; show vlan &lt;id&gt;</td>
<td>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</td>
</tr>
<tr>
<td>Add a SNIP address.</td>
<td>add nsip &lt;IPAddress&gt; &lt;netmask&gt; -type SNIP; show nsip</td>
<td>add nsip 198.51.100.18 255.255.255.0 -type SNIP; add nsip 198.51.101.18 255.255.255.0 -type SNIP</td>
</tr>
<tr>
<td>Create services representing HTTP servers.</td>
<td>add service &lt;serviceName&gt; &lt;ip&gt; HTTP &lt;port&gt;; show service &lt;name&gt;</td>
<td>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</td>
</tr>
<tr>
<td>Create HTTP load balancing virtual servers and bind the services to it</td>
<td>add lb vserver &lt;name&gt; HTTP &lt;ip&gt; &lt;port&gt;; bind lb vserver &lt;vserverName&gt; &lt;serviceName&gt;; show lb vserver &lt;name&gt;</td>
<td>add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1; bind lb vserver LBVS-1 SVC-S2 add lb vserver LBVS-2 http 203.0.114.15 80; bind lb vserver LBVS-2 SVC-S3; bind lb vserver LBVS-2 SVC-S4</td>
</tr>
<tr>
<td>Create a custom TCP profile and set its MSS for supporting jumbo frames.</td>
<td>add tcpProfile &lt;name&gt; -mss &lt;positive_integer&gt;; show tcpProfile &lt;name&gt;</td>
<td>add tcpProfile ALL-JUMBO -mss 8960</td>
</tr>
</tbody>
</table>
**Task Syntax Example**

Bind the custom TCP profile to the desired load balancing virtual server and services.

```
set service <Name> -tcpProfileName <string>;
show service <name>
```

Set load balancer 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
```

---

**Configure SNMP on SDX appliances**

October 16, 2019

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

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

The following figure illustrates a network with a 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 SDX appliance.

*Figure 1. SDX Appliance Supporting SNMP*
The SNMP agent on the SDX appliance generates traps that are compliant with SNMPv2 only. The supported traps can be viewed in the SDX MIB file. You can download this file from the Downloads page in the SDX user interface.

**To add an SNMP trap destination**

1. On the configuration tab, in the navigation pane, expand System > 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 (.), 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 SNMPTapDestinations pane, select the trap destination that you want to modify, and then click Modify. In the ModifySNMP Trap Destination dialog box, modify the parameters.

To remove an SNMP trap, in the SNMPTapDestinations 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.

**Download MIB files**

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

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

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

**To download MIB files**

1. Log on to the Downloads page of the SDX appliance user interface.
2. Under SNMP Files, click SNMPv2 - MIB Object Definitions. You can open the file by using a MIB browser.

**Add an SNMP manager community**

You must configure SNMP managers on the SDX appliance to query and monitor the appliance and managed devices hosted on the appliance. Also, you must 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 Community page, 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.
   - Select the **Enable Management Network** checkbox to specify the SNMP managers by using the netmask.
   - In the **Netmask** field, enter the netmask of the SNMP community.

5. Click Add, and then click Close.

Configure the SDX appliance for SNMPv3 queries

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 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.

Add an SNMP manager

You must configure the 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. 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.

### Configure an SNMP view

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.

### Configure an SNMP user

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 User page, 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.

Configure an SNMP alarm

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

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

- Critical
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.

**Configure syslog notifications**

January 23, 2019

SYSLOG is a standard logging protocol. It has two components: the SYSLOG auditing module, which runs on the Citrix NetScaler 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 timestamp
- The message type
- The log level (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- The message information

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

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

To configure the syslog parameters

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

Configure mail notifications

January 23, 2019

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 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.
Configure SMS notifications

January 23, 2019

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 Server page, 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.

Monitor and manage the real-time status of entities configured on an SDX appliance

January 23, 2019

The Citrix NetScaler SDX appliance can monitor and manage the states of virtual servers, services, service groups, and servers across the virtual appliances hosted on the SDX appliance. 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 Citrix NetScaler instances.
View 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 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
     - IPAddress—IP address of the virtual server. Clients send connection requests to this IP address.
     - Port—Port on which the virtual server listens for client connections.
     - Last State Change—Elapsed time (in days, hours, minutes, and seconds) since the last change in the state of the virtual server, that is, the duration of time for which the virtual server has been in the current state. This information is available only for virtual
servers configured on NetScaler release 9.0 and later.

- **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.
View the status of services

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

To view the status of virtual servers

1. On the Configuration tab, in the navigation pane, click NetScaler > Entities > Service.
2. In the details pane, under Services, view the following statistics:
   - Device Name—Name of the device on which the service is configured.
   - Name—Name of the service.
   - Protocol—Service type, which determines the behavior of the service. For example, HTTP, TCP, UDP, or SSL.
   - State—Current state of the service. For example, UP, DOWN, or OUT OF SERVICE.
   - IP Address—IP address of the service.
   - Port—Port on which the service listens.
   - Last State Change—Elapsed time (in days, hours, minutes, and seconds) since the last change in the state of the service, that is, the duration of time for which the service has been in the current state.

• Viewing the Virtual Servers to which a Service is Bound

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

To view the virtual servers to which a service is bound

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

You can monitor the real-time state of a service group member from the 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 Citrix 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.

Configure the polling interval

You can set the time interval for which you want the 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 SDX must poll the entity value. Minimum value of the polling interval is 30 minutes. Click OK.

Monitor and manage events generated on Citrix netScaler instances
Use the Events feature to monitor and manage the events generated on the Citrix NetScaler instances. The Management Service identifies events in real time, thereby helping you address issues immediately and keep the Citrix 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.

**View all events**

You can view all the events generated on the Citrix NetScaler instances provisioned on the Citrix 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. |

**View 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 Citrix NetScaler instances by All Events**

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

**Top 10 Citrix NetScaler instances by Entity State Change Events**

This report is a bar chart that displays the top 10 Citrix 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 Citrix NetScaler instances by Threshold Violation Events**

This report is a bar chart that displays the top 10 Citrix 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 Citrix NetScaler instances by Hardware Failure Events**

This report is a bar chart that displays the top 10 Citrix 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 Citrix NetScaler instances by Configuration Change Events**

This report is a bar chart that reflects the top 10 Citrix 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 Citrix NetScaler instances by Authentication Failure Events**

This report is a bar chart that displays the top 10 Citrix 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 Citrix NetScaler instances for which you want to define a event rule.
- Category—Category or categories of the events generated by the Citrix NetScaler instances.
- Failure Objects—Entity instances or counters for which an event has been generated.

3. Click Save.

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

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.
b) 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 Citrix NetScaler instances on the 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 Citrix NetScaler instances for which you want to suppress this event by using the Advanced option.
4. Click OK.

**Call Home support for Citrix NetScaler instances on an SDX appliance**

January 23, 2019

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

Note: The Citrix 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 Citrix NetScaler instance initiates the registration process.

- **Enabling and Disabling Call Home on a Citrix NetScaler instance**

  You can enable the Call Home feature on Citrix NetScaler instance from the Management Service. When you enable the Call Home feature, the Call Home process registers the Citrix 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 Citrix 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 Citrix 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 Citrix NetScaler instance’s data to the Citrix TaaS server through a proxy server. To use this feature, enable it on your Citrix 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 Citrix 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 Citrix NetScaler instance, navigate to Configuration > NetScaler > Call Home, select the Citrix NetScaler instance and click Configure button. In the Configure Call Home page, click OK.

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

- Polling the Citrix NetScaler instances

To poll the Call Home feature from all Citrix 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

January 23, 2019

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 Citrix 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.
Monitor the resources on the SDX appliance

You can monitor the hardware and software components on the 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.

Monitor the storage resources on the SDX appliance

You can monitor the disks on the 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).

**Monitor the hardware sensors on the SDX appliance**

You can monitor the hardware components on the SDX appliance and take corrective action if required. In the Monitoring tab, expand System Health, and then click Hardware Sensors. The mon-
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.
Monitor the interfaces on the SDX appliance

You can monitor the interfaces on the 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.

Configure system notification settings

January 23, 2019

You can send notifications to communicate with select groups of users for a number of system-related functions. You can set up a notification server in SDX Management Service to configure email and Short Message Service (SMS) gateway servers to send email and text (SMS) notifications to users.
To configure system notification settings

1. Navigate to System > Notifications > Settings, and then click Change Notification Settings.

2. In the Configure System Notification Settings page, enter the following details:
   - **Category** – Category or categories of the events generated by the SDX Management Service.
   - **Email** – Select an email distribution list from the drop-down menu. You can also create a new email distribution list by clicking on the + icon and entering the new email server details in the appropriate fields.
   - **SMS (Text Message)** – Select an SMS distribution list from the drop-down menu. You can also create a new SMS distribution list by clicking on the + icon and entering the new SMS server details in the appropriate fields.

3. Click OK.

Configuring the Management Service

January 23, 2019

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. And, using the backup policy, you can:

• Encrypt the backup files.
• Configure the SDX appliance to transfer the backup files to an external backup server using FTP, SFTP, and SCP.

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 configure the backup policy:**

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. Select **Encrypt Backup File** to encrypt the backup file.
5. Select **External Transfer** and do the following to transfer the backup file to an external backup server:
   a) In the **Server** field, enter hostname or IP address of the external backup server.
   b) In the **User Name** and **Password** fields, enter the username and password to access the external backup server.
   c) In the **Port** field, enter the port number.
   d) In the **Transfer Protocol** field, select the protocol you want to use to transfer the backup file to the external backup server.
   e) In the **Directory Path** field, enter the path of the directory in the external backup server where you want to store the backup files.
6. Select **Delete file from Management Service after transfer** if you want to delete the backup file from the SDX appliance after you have transferred the backup file to the external backup server.
7. 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**

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 Citrix 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

March 24, 2020

Authentication with the Citrix NetScaler SDX Management Service can be local or external. With external authentication, the Management Service grants user access based on 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 read-only 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 read-only privileges are allowed to perform only read operations. The authorization of SSH users is limited to admin privileges only. Users with read-only 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 read-only privileges. When a user logs on to 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 read-only 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 users.

If you are using external authentication servers for authentication, groups in 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 SDX appliance.

**To add a user group**

1. On the **Configuration** tab, under **System**, expand **User Administration**, and then click **Groups**.
2. In the details pane, click **Add**.
3. In the Create System Group page, set the following parameters:

- Group Name
- Group Description
- System Access: Select this box to give access to the entire SDX appliance and the instances running on it. Alternatively, for instance-level access, specify the instances under Instances.
- Permission
- Configure User Session Timeout
- Users: Database users belonging to the Group. Select the users you want to add to the group.

4. Click Create and Close
To create a group with admin role on an SDX appliance that is upgraded from version 10.5 to 11.1, select the “read-write” permission and “System Access” check box. In SDX 10.5, this check box is not available and the values for Permission are “admin” and “read-only”.

### Configuring User Accounts

A user logs on to the 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 username 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.
     - read-only—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

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

January 23, 2019

The Citrix NetScaler SDX 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 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.
   - Server Name / IP Address*—FQDN or Server IP address.
     Note: DNS should be able to resolve the specified fully qualified domain name (FQDN) to an IP address, and only the primary DNS is used to resolve the FQDN. To manually set the primary DNS, see the section “Adding a Primary DNS for FQDN Name Resolution.”
   - 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 IPAddress 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.
   - IPAddress 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.
   - Server Name / IP Address*—FQDN or Server IP address.
     **Note:** DNS should be able to resolve the specified FQDN to an IP address, and only the primary DNS is used to resolve the FQDN. To manually set the primary DNS, see the section “Adding a Primary DNS for FQDN Name Resolution.”
   - 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: (&(vpnal-lowed=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
NetScaler SDX 11.1

- 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.

**SSH public key authentication support for LDAP users**

The SDX appliance can now authenticate the LDAP users through SSH public key authentication for logon. The list of public keys is stored on the user object in the LDAP server. During authentication, SSH extracts the SSH public keys from the LDAP server. The logon succeeds if any of the retrieved public key works with SSH.

The same attribute name of the extracted public key must be present in both LDAP server and in the Citrix NetScaler SDX appliance.

**Important**

For key-based authentication, you must specify a location of the public keys by setting the value of `Authorizedkeysfile` in `/etc/sshd_config` file in the following aspect:

```
AuthorizedKeysFile .ssh/authorized_keys
```

**System User.** You can specify the location of public keys for any system user by setting the value of `Authorizedkeysfile` in `/etc/sshd_config` file.

**LDAP Users.** The retrieved public key is stored in the `/var/pubkey/<user_name>/tmpAuthorized_keys-<pid>`. The `<pid>` is the unique number added to differentiate between concurrent SSH requests from the same user. This is the temporary location to hold the public key during the authentication process. The public key is removed from the system once authentication is complete.

To login with the user, run the following command from the shell prompt:
To configure LDAP server by using the GUI:

1. Navigate to **System > Authentication > LDAP**.
2. On the LDAP page, click **Servers** tab.
3. Click any of the available LDAP servers.
4. On the **Configure Authentication LDAP Server** page, check the **Authentication** checkbox for authentication purpose.

**Note**

Uncheck the Authentication check box to use “sshPublicKeys” for authentication of LDAP users.

Adding a Primary DNS for FQDN Name Resolution

If you define a RADIUS or an LDAP server by using the FQDN of the server rather than its IP address, you must manually set the primary DNS to resolve the server name, either by using the GUI or CLI.

To set the primary DNS by using the GUI, go to **System > Network Configuration > DNS**.

To set the primary DNS by using the CLI, follow these steps.

1. Open a Secure Shell (SSH) console.
2. Log on to the Citrix NetScaler SDX appliance by using the nsroot/nsroot credentials.
3. Run the networkconfig command.
4. Select the appropriate menu and update the DNS IPv4 Address, and save the changes.

If you run the networkconfig command again, you’ll see the updated DNS address.

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

$ ssh -i <privatekey> <username>@<IPAddress>
• 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

January 23, 2019

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 Citrix NetScaler SDX 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 Citrix 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**

January 23, 2019

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 Citrix NetScaler instance or later at the time of modifying a Citrix 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 Citrix NetScaler SDX 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.

**Set up a cluster of Citrix ADC instances**

January 11, 2019

After provisioning Citrix ADC instances on one or more SDX appliances, you can create a cluster of Citrix ADC instances. The nodes of the cluster can be Citrix ADC 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 Citrix ADC clustering. For more information, see Clustering.
- For clusters that have Citrix ADC instances across SDX appliances, Citrix recommends that you use Citrix ADC instances from three SDX appliances. This ensures that the cluster criteria of a minimum of (n/2 +1) nodes is always satisfied.

Figure 1. Cluster of SDX Citrix ADC instances
The above figure shows three SDX appliances, SDX1, SDX2, and SDX3, on the same subnet. The Citrix ADC 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 Citrix ADC instances and SDX Citrix ADC instances.
- The Citrix ADC instances must be of the same version, which must be version 10.1 or later.
- The Citrix ADC instances must all have the same feature license.
- No configurations can be updated on individual Citrix ADC instances after they are added to the cluster. All changes must be performed through the cluster IP address.
- The Citrix ADC instances must all have the same resources (memory, CPU, interfaces, and so on).

**To set up a cluster on an SDX appliance**

1. Log on to the SDX appliance.
2. On the Configuration tab, navigate to Citrix ADC, and then click Clusters.
3. Create the cluster:
   a) Click Create Cluster.
   b) 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.
   c) Click Next to view the configuration summary.
   d) Click Finish to create the cluster.

Note: When a Citrix ADC instance that is provisioned on the 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:
   a) Click Add Node.
   b) 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.
   c) Click Next to view the configuration summary.
   d) Click Finish to add the node to the cluster.
   e) 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 Citrix ADC clusters, each of which has at least one Citrix ADC instance of the SDX appliance, use the Rediscover option.

To add a Citrix ADC 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 Citrix ADC instance.
2. On the Configuration tab, navigate to Citrix ADC, 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 SSL Ciphers to Securely Access the Management Service

July 3, 2019

You can select SSL cipher suites from a list of SSL ciphers supported by Citrix NetScaler SDX appliances, and bind any combination of the SSL ciphers to access the SDX 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.
NetScaler SDX 11.1

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.

<table>
<thead>
<tr>
<th>Citrix Cipher Name</th>
<th>Openssl CipherName</th>
<th>Hex Code</th>
<th>Protocol</th>
<th>KeyExchange</th>
<th>Auth</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS1-AES-256-CBC-SHA</td>
<td>AES256-SHA</td>
<td>0x0035</td>
<td>SSLv3</td>
<td>RSA</td>
<td>RSA</td>
<td>AES(256)</td>
</tr>
<tr>
<td>TLS1-AES-128-CBC-SHA</td>
<td>AES128-SHA</td>
<td>0x002F</td>
<td>SSLv3</td>
<td>RSA</td>
<td>RSA</td>
<td>AES(128)</td>
</tr>
<tr>
<td>TLS1.2-AES-256-SHA256</td>
<td>AES256-SHA256</td>
<td>0x003D</td>
<td>TLSv1.2</td>
<td>RSA</td>
<td>RSA</td>
<td>AES(256)</td>
</tr>
<tr>
<td>TLS1.2-AES-128-SHA256</td>
<td>AES128-SHA256</td>
<td>0x003C</td>
<td>TLSv1.2</td>
<td>RSA</td>
<td>RSA</td>
<td>AES(128)</td>
</tr>
<tr>
<td>TLS1.2-AES256-GCM-SHA384</td>
<td>AES256-GCM-SHA384</td>
<td>0x009D</td>
<td>TLSv1.2</td>
<td>RSA</td>
<td>RSA</td>
<td>AES-GCM(256)</td>
</tr>
<tr>
<td>TLS1.2-AES128-GCM-SHA256</td>
<td>AES128-GCM-SHA256</td>
<td>0x009C</td>
<td>TLSv1.2</td>
<td>RSA</td>
<td>RSA</td>
<td>AES-GCM(128)</td>
</tr>
<tr>
<td>TLS1-ECDHE-RSA-AES256-SHA</td>
<td>ECDHE-RSA-AES256-SHA</td>
<td>0xC014</td>
<td>SSLv3</td>
<td>ECC-DHE</td>
<td>RSA</td>
<td>AES(256)</td>
</tr>
<tr>
<td>Citrix Cipher Name</td>
<td>Openssl CipherName</td>
<td>Hex Code</td>
<td>Protocol</td>
<td>KeyExchange</td>
<td>Auth</td>
<td>MAC</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>TLS1.2-ECDHE-RSA-AES128-SHA</td>
<td>ECDHE-RSA-AES128-SHA</td>
<td>0xC013</td>
<td>SSLv3</td>
<td>ECC-DHE</td>
<td>RSA</td>
<td>AES(128)</td>
</tr>
<tr>
<td>TLS1.2-ECDHE-RSA-AES256-SHA384</td>
<td>ECDHE-RSA-AES256-SHA384</td>
<td>0xC028</td>
<td>TLSv1.2</td>
<td>ECC-DHE</td>
<td>RSA</td>
<td>AES(256)</td>
</tr>
<tr>
<td>TLS1.2-ECDHE-RSA-AES128-SHA256</td>
<td>ECDHE-RSA-AES128-SHA256</td>
<td>0xC027</td>
<td>TLSv1.2</td>
<td>ECC-DHE</td>
<td>RSA</td>
<td>AES(128)</td>
</tr>
<tr>
<td>TLS1.2-ECDHE-RSA-AES256-GCM-SHA384</td>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
<td>0xC030</td>
<td>TLSv1.2</td>
<td>ECC-DHE</td>
<td>RSA</td>
<td>AES-GCM(256)</td>
</tr>
<tr>
<td>TLS1.2-ECDHE-RSA-AES128-GCM-SHA256</td>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td>0xC02F</td>
<td>TLSv1.2</td>
<td>ECC-DHE</td>
<td>RSA</td>
<td>AES-GCM(128)</td>
</tr>
<tr>
<td>TLS1.2-DHE-RSA-AES256-SHA256</td>
<td>DHE-RSA-AES256-SHA256</td>
<td>0x006B</td>
<td>TLSv1.2</td>
<td>DH</td>
<td>RSA</td>
<td>AES(256)</td>
</tr>
<tr>
<td>TLS1.2-DHE-RSA-AES128-SHA256</td>
<td>DHE-RSA-AES128-SHA256</td>
<td>0x0067</td>
<td>TLSv1.2</td>
<td>DH</td>
<td>RSA</td>
<td>AES(128)</td>
</tr>
<tr>
<td>Citrix Cipher Name</td>
<td>Openssl CipherName</td>
<td>Hex Code</td>
<td>Protocol</td>
<td>KeyExchange</td>
<td>Auth</td>
<td>MAC</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------</td>
<td>----------------</td>
</tr>
<tr>
<td>TLS1.2-DHE-RSA-AES256-GCM-SHA384</td>
<td>DHE-RSA-AES256-GCM-SHA384</td>
<td>0x009F</td>
<td>TLSv1.2</td>
<td>DH</td>
<td>RSA</td>
<td>AES-GCM(256)</td>
</tr>
<tr>
<td>TLS1.2-DHE-RSA-AES128-GCM-SHA256</td>
<td>DHE-RSA-AES128-GCM-SHA256</td>
<td>0x009E</td>
<td>TLSv1.2</td>
<td>DH</td>
<td>RSA</td>
<td>AES-GCM(128)</td>
</tr>
<tr>
<td>TLS1-DHE-RSA-AES256-CBC-SHA</td>
<td>DHE-RSA-AES256-SHA</td>
<td>0x0039</td>
<td>SSLv3</td>
<td>DH</td>
<td>RSA</td>
<td>AES(256)</td>
</tr>
<tr>
<td>TLS1-DHE-RSA-AES128-CBC-SHA</td>
<td>DHE-RSA-AES128-SHA</td>
<td>0x0033</td>
<td>SSLv3</td>
<td>DH</td>
<td>RSA</td>
<td>AES(128)</td>
</tr>
<tr>
<td>TLS1-DHE-DSS-AES256-CBC-SHA</td>
<td>DHE-DSS-AES256-SHA</td>
<td>0x0038</td>
<td>SSLv3</td>
<td>DH</td>
<td>DSS</td>
<td>AES(256)</td>
</tr>
<tr>
<td>TLS1-DHE-DSS-AES128-CBC-SHA</td>
<td>DHE-DSS-AES128-SHA</td>
<td>0x0032</td>
<td>SSLv3</td>
<td>DH</td>
<td>DSS</td>
<td>AES(128)</td>
</tr>
<tr>
<td>TLS1-ECDHE-RSA-DES-CBC3-SHA</td>
<td>ECDHE-RSA-DES-CBC3-SHA</td>
<td>0xC012</td>
<td>SSLv3</td>
<td>ECC-DHE</td>
<td>RSA</td>
<td>3DES(168)</td>
</tr>
<tr>
<td>SSL3-EDH-RSA-DES-CBC3-SHA</td>
<td>EDH-RSA-DES-CBC3-SHA</td>
<td>0x0016</td>
<td>SSLv3</td>
<td>DH</td>
<td>RSA</td>
<td>3DES(168)</td>
</tr>
<tr>
<td>Citrix Cipher Name</td>
<td>Openssl CipherName</td>
<td>Hex Code</td>
<td>Protocol</td>
<td>KeyExchange</td>
<td>Auth</td>
<td>MAC</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>SSL3-EDH-DSS-DES-CBC3-SHA</td>
<td>EDH-DSS-DES-CBC3-SHA</td>
<td>0x0013</td>
<td>SSLv3</td>
<td>DH</td>
<td>DSS</td>
<td>3DES(168)</td>
</tr>
<tr>
<td>TLS1-ECDHE-RSA-RC4-SHA</td>
<td>ECDHE-RSA-RC4-SHA</td>
<td>0xC011</td>
<td>SSLv3</td>
<td>ECC-DHE</td>
<td>RSA</td>
<td>RC4(128)</td>
</tr>
<tr>
<td>SSL3-DES-CBC3-SHA</td>
<td>DES-CBC3-SHA</td>
<td>0x000A</td>
<td>SSLv3</td>
<td>RSA</td>
<td>RSA</td>
<td>3DES(168)</td>
</tr>
<tr>
<td>SSL3-RC4-SHA</td>
<td>RC4-SHA</td>
<td>0x0005</td>
<td>SSLv3</td>
<td>RSA</td>
<td>RSA</td>
<td>RC4(128)</td>
</tr>
<tr>
<td>SSL3-RC4-MD5</td>
<td>RC4-MD5</td>
<td>0x0004</td>
<td>SSLv3</td>
<td>RSA</td>
<td>RSA</td>
<td>RC4(128)</td>
</tr>
<tr>
<td>SSL3-DES-CBC-SHA</td>
<td>DES-CBC-SHA</td>
<td>0x0009</td>
<td>SSLv3</td>
<td>RSA</td>
<td>RSA</td>
<td>DES(56)</td>
</tr>
<tr>
<td>SSL3-EXP-RC4-MD5</td>
<td>EXP-RC4-MD5</td>
<td>0x0003</td>
<td>SSLv3</td>
<td>RSA(512)</td>
<td>RSA</td>
<td>RC4(40)</td>
</tr>
<tr>
<td>SSL3-EXP-DES-CBC-SHA</td>
<td>EXP-DES-CBC-SHA</td>
<td>0x0008</td>
<td>SSLv3</td>
<td>RSA(512)</td>
<td>RSA</td>
<td>DES(40)</td>
</tr>
<tr>
<td>SSL3-EXP-RC2-CBC-MD5</td>
<td>EXP-RC2-CBC-MD5</td>
<td>0x0006</td>
<td>SSLv3</td>
<td>RSA(512)</td>
<td>RSA</td>
<td>RC2(40)</td>
</tr>
<tr>
<td>SSL2-DES-CBC-MD5</td>
<td>DHE-DSS-AES128-SHA256</td>
<td>0x0040</td>
<td>SSLv2</td>
<td>RSA</td>
<td>RSA</td>
<td>DES(56)</td>
</tr>
<tr>
<td>SSL3-EDH-DSS-DES-CBC-SHA</td>
<td>EDH-DSS-DES-CBC-SHA</td>
<td>0x0012</td>
<td>SSLv3</td>
<td>DH</td>
<td>DSS</td>
<td>DES(56)</td>
</tr>
<tr>
<td>SSL3-EXP-EDH-DSS-DES-CBC-SHA</td>
<td>EXP-EDH-DSS-DES-CBC-SHA</td>
<td>0x0011</td>
<td>SSLv3</td>
<td>DH(512)</td>
<td>DSS</td>
<td>DES(40)</td>
</tr>
<tr>
<td>Citrix Cipher Name</td>
<td>Openssl Cipher Name</td>
<td>Hex Code</td>
<td>Protocol</td>
<td>Key Exchange</td>
<td>Auth</td>
<td>MAC</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------</td>
<td>----------</td>
<td>----------</td>
<td>--------------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>SSL3-EDH-RSA-DES-CBC-SHA</td>
<td>EDH-RSA-DES-CBC-SHA</td>
<td>0x0015</td>
<td>SSLv3</td>
<td>DH</td>
<td>RSA</td>
<td>DES(56)</td>
</tr>
<tr>
<td>SSL3-EXP-EDH-RSA-DES-CBC-SHA</td>
<td>EXP-EDH-RSA-DES-CBC-SHA</td>
<td>0x0014</td>
<td>SSLv3</td>
<td>DH(512)</td>
<td>RSA</td>
<td>DES(40)</td>
</tr>
<tr>
<td>SSL3-ADH-RC4-MD5</td>
<td>ADH-RC4-MD5</td>
<td>0x0018</td>
<td>SSLv3</td>
<td>DH</td>
<td>None</td>
<td>RC4(128)</td>
</tr>
<tr>
<td>SSL3-ADH-DES-CBC3-SHA</td>
<td>ADH-DES-CBC3-SHA</td>
<td>0x001B</td>
<td>SSLv3</td>
<td>DH</td>
<td>None</td>
<td>3DES(168)</td>
</tr>
<tr>
<td>SSL3-ADH-DES-CBC-SHA</td>
<td>ADH-DES-CBC-SHA</td>
<td>0x001A</td>
<td>SSLv3</td>
<td>DH</td>
<td>None</td>
<td>DES(56)</td>
</tr>
<tr>
<td>TLS1-ADH-AES-128-CBC-SHA</td>
<td>ADH-AES128-SHA</td>
<td>0x0034</td>
<td>SSLv3</td>
<td>DH</td>
<td>None</td>
<td>AES(128)</td>
</tr>
<tr>
<td>TLS1-ADH-AES-256-CBC-SHA</td>
<td>ADH-AES256-SHA</td>
<td>0x003A</td>
<td>SSLv3</td>
<td>DH</td>
<td>None</td>
<td>AES(256)</td>
</tr>
<tr>
<td>SSL3-EXP-ADH-RC4-MD5</td>
<td>EXP-ADH-RC4-MD5</td>
<td>0x0017</td>
<td>SSLv3</td>
<td>DH(512)</td>
<td>None</td>
<td>RC4(40)</td>
</tr>
<tr>
<td>SSL3-EXP-ADH-DES-CBC-SHA</td>
<td>EXP-ADH-DES-CBC-SHA</td>
<td>0x0019</td>
<td>SSLv3</td>
<td>DH(512)</td>
<td>None</td>
<td>DES(40)</td>
</tr>
<tr>
<td>SSL3-NULL-MD5</td>
<td>NULL-MD5</td>
<td>0x0001</td>
<td>SSLv3</td>
<td>RSA</td>
<td>RSA</td>
<td>None</td>
</tr>
<tr>
<td>SSL3-NULL-SHA</td>
<td>NULL-SHA</td>
<td>0x0002</td>
<td>SSLv3</td>
<td>RSA</td>
<td>RSA</td>
<td>None</td>
</tr>
</tbody>
</table>
## Predefined Cipher Groups

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

<table>
<thead>
<tr>
<th>Cipher Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>All ciphers supported by the SDX appliance, excluding NULL ciphers</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>Default cipher list with encryption strength $\geq$ 128bit</td>
</tr>
<tr>
<td>kRSA</td>
<td>Ciphers with Key-ex algo as RSA</td>
</tr>
<tr>
<td>kEDH</td>
<td>Ciphers with Key-ex algo as Ephemeral-DH</td>
</tr>
<tr>
<td>DH</td>
<td>Ciphers with Key-ex algo as DH</td>
</tr>
<tr>
<td>EDH</td>
<td>Ciphers with Key-ex/Auth algo as DH</td>
</tr>
<tr>
<td>aRSA</td>
<td>Ciphers with Auth algo as RSA</td>
</tr>
<tr>
<td>aDSS</td>
<td>Ciphers with Auth algo as DSS</td>
</tr>
<tr>
<td>aNULL</td>
<td>Ciphers with Auth algo as NULL</td>
</tr>
<tr>
<td>DSS</td>
<td>Ciphers with Auth algo as DSS</td>
</tr>
<tr>
<td>DES</td>
<td>Ciphers with Enc algo as DES</td>
</tr>
<tr>
<td>3DES</td>
<td>Ciphers with Enc algo as 3DES</td>
</tr>
<tr>
<td>RC4</td>
<td>Ciphers with Enc algo as RC4</td>
</tr>
<tr>
<td>RC2</td>
<td>Ciphers with Enc algo as RC2</td>
</tr>
<tr>
<td>NULL</td>
<td>Ciphers with Enc algo as NULL</td>
</tr>
<tr>
<td>MD5</td>
<td>Ciphers with MAC algo as MD5</td>
</tr>
<tr>
<td>SHA1</td>
<td>Ciphers with MAC algo as SHA-1</td>
</tr>
<tr>
<td>SHA</td>
<td>Ciphers with MAC algo as SHA</td>
</tr>
<tr>
<td>NULL</td>
<td>Ciphers with Enc algo as NULL</td>
</tr>
<tr>
<td>RSA</td>
<td>Ciphers with Key-ex/Auth algo as RSA</td>
</tr>
<tr>
<td>ADH</td>
<td>Ciphers with Key-ex algo as DH and Auth algo as NULL</td>
</tr>
<tr>
<td>SSLv2</td>
<td>SSLv2 protocol ciphers</td>
</tr>
<tr>
<td>SSLv3</td>
<td>SSLv3 protocol ciphers</td>
</tr>
<tr>
<td>TLSv1</td>
<td>SSLv3/TLSv1 protocol ciphers</td>
</tr>
<tr>
<td>Cipher Group Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>TLSv1_ONLY</td>
<td>TLSv1 protocol ciphers</td>
</tr>
<tr>
<td>EXP</td>
<td>Export ciphers</td>
</tr>
<tr>
<td>EXPORT</td>
<td>Export ciphers</td>
</tr>
<tr>
<td>EXPORT40</td>
<td>Export ciphers with 40bit encryption</td>
</tr>
<tr>
<td>EXPORT56</td>
<td>Export ciphers with 56bit encryption</td>
</tr>
<tr>
<td>LOW</td>
<td>Low strength ciphers (56bit encryption)</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Medium strength ciphers (128bit encryption)</td>
</tr>
<tr>
<td>HIGH</td>
<td>High strength ciphers (168bit encryption)</td>
</tr>
<tr>
<td>AES</td>
<td>AES Ciphers</td>
</tr>
<tr>
<td>FIPS</td>
<td>FIPS Approved Ciphers</td>
</tr>
<tr>
<td>ECDHE</td>
<td>Elliptic Curve Ephemeral DH Ciphers</td>
</tr>
<tr>
<td>AES-GCM</td>
<td>Ciphers with Enc algo as AES-GCM</td>
</tr>
<tr>
<td>SHA2</td>
<td>Ciphers with MAC algo as SHA-2</td>
</tr>
</tbody>
</table>

**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:
   a) In the **Group Name** field, enter a name for the custom cipher group.
   b) In the **Cipher Group Description** field, enter a brief description of the custom cipher group.
   c) In the **Cipher Suites** section, click **Add** and select the ciphers to include in the list of supported SSL ciphers.
d) 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 **Configure 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 **Configure 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**.
NetScaler SDX 11.1

Backing Up and Restoring the Configuration Data of the SDX Appliance

January 23, 2019

The Citrix 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
- XVA image
- Upgrade image
- SDX configuration
- Configuration

To back up 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, type and confirm the password for the backup file.
5. Click Continue.

The backup process creates a backup file. The file name of the backup file includes the current IP address of the Management Service and the timestamp when the backup was taken. To check for any discrepancy that the backup file might have, from the SDX GUI navigate to Configuration > System > Events/Alarms.

Scheduled Backup

By default, 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. 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:
NetScaler SDX 11.1

a) In the Previous backups to retain field, type the number of backup files you want to retain.
b) To encrypt the backup files, select Encrypt Backup File check box.
c) In the Password and Confirm Password fields, type and confirm the password to encrypt the backup file.

Manually Transfer the Backup File to an External Backup Server

You can manually transfer the backup file to an external backup server. Ensure 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, type hostname or IP address of the external backup server.
4. In the User Name and Password fields, type the user name and password to access the external backup server.
5. In the Port field, type 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, type 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 transferred the backup file to the external backup server.
9. Click OK.

Restoring the Appliance

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

**Points to note**

- If you restore the SDX appliance using the backup file of a different SDX appliance, ensure that you add the configure Management Service network settings in the appliance according to the settings available in the backup file, before you start the restore process.
- Ensure that the platform variant on which the backup was taken is same as on which you are trying to restore (restoring the backup file between two 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, click the backup file and then click OK.

3. In the Restore dialog box, select Appliance Restore, and then click Proceed.

A page appears showing the different components of the application restore:

- License
- SDX Image
- XVA Files
- Citrix NetScaler configuration
- Summary

If any of the required components such as a valid and capable license, XVA images, Citrix NetScaler images, Single Bundle image are missing in the backup file, you’re prompted to upload the missing element before proceeding further.

To know whether a backup file can be restored on the current SDX Single Bundle Image Version, see this table.

<table>
<thead>
<tr>
<th>Current SDX Single Bundle Image Version</th>
<th>Backup File Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>supported on 11.0, 12.0</td>
</tr>
<tr>
<td>11.1</td>
<td>supported on 11.1, 12.0; not supported on 11.0</td>
</tr>
<tr>
<td>12.0</td>
<td>supported on 12.0; not supported on 11.0 and 11.1</td>
</tr>
</tbody>
</table>
4. On the License page, check that a valid license is present and click Next.

5. The SDX Image page appears. If an SDX image is not required to perform the restore, click Next. Otherwise, when prompted upload a valid SDX image and click Next.

6. The XVA File page opens. Click Next if XVA images for all instances are present. If the XVA file for any instance is missing in the backup file, you can either upload it or skip restoring this instance. Click Next to go to the next page.

7. The NetScaler Configuration page opens. NetScaler configuration files are not mandatory. You can provision the instance without restoring its configuration. If the NetScaler configuration file is missing in the backup file, you can either proceed only with instance provisioning or skip restoring the instance. Click Next to go to the next page.

8. The summary page appears with the following details about all the instances present in the backup file:
   - IP address
   - Hostname
   - SDX version
   - XVA version
   - Version bit
   - Restore: if the appliance or instance is ready for restore, a check mark appears. If it’s not, a cross mark appears.
• Error messages: if the appliance or instance is not ready for restore, an error message appears explaining the reason.

9. Click **Restore** to complete the application restore process.

**Restoring the Citrix NetScaler instance**

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

**Points to note:**

• A VPX instance fails to restore if the instance does not have any management NIC assigned to it and if the instance is managed from the SDX Management Service only through LACP. The restore fails because SDX Management Service cannot restore the channel configurations automatically. To avoid this issue, manually restore the channel configuration to complete the VPX instance restore.

To restore the Citrix 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 Citrix NetScaler instances that you want to restore and then click **Proceed**.
5. (Optional) If the backup file is encrypted, when prompted, type the password and then click **OK**.

**Note**

Ensure that appropriate XVA, build image, and channel configuration are present on the SDX appliance that runs the instance that is being restored.

**Performing Appliance Reset**

July 17, 2019

The Citrix 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 Citrix 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 following options to reset the Appliance:

- Config Reset
- Factory Reset
- Clean Install

### Resetting the Configuration of the Appliance

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

- Deletes 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.
- Deletes the Citrix NetScaler SDX image.
- Deletes all XVA images except the last image file that was accessed on the appliance.
- Restores default interface settings.
- Restores the default configuration of the appliance, including default profiles, users, and system settings.
- Restores default IP addresses for XenServer and the Management Service.
- Restores default passwords for XenServer and the Management Service.
- Restarts the Management Service.

**To reset the configuration of the Appliance:**

1. Under **Configuration** tab, click the **System** node and then under the **System Administration** group, click **Appliance Reset**.
2. In the **Appliance Reset** dialog box, select **Config Reset** in the **Reset Type** drop-down list, and click **OK**.

### Resetting the Appliance to Factory Version

The Management Service provides the Factory Reset option to reset the appliance to the factory version. The Factory Reset option resets the current IP addresses of the Management Service and
XenServer to the default IP addresses of the Management Service and XenServer.

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

**Important**

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

**To reset the Appliance to factory version:**

1. Under **Configuration** tab, click **System** node and then under the **System Administration** group, click **Appliance Reset**.
2. In the **Appliance Reset** dialog box, select **Factory Reset** in the **Reset Type** drop-down list, and click **OK**.

**Resetting the Appliance to a Single Bundle Image Version**

The Management Service provides the Clean Install option that allows you to install an arbitrary version of single bundle image on the appliance. It enables you to perform fresh install of the single bundle image as the new default boot image. Clean installation removes the existing configuration, except network settings, in the SDX appliance.

The clean-install option is supported on the following:

<table>
<thead>
<tr>
<th>Single Bundle Image Version</th>
<th>SDX Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0.xx</td>
<td>SDX 14xxx, SDX 25xxx. <strong>Note:</strong> The clean-install option is supported on other SDX platforms if they have 10G factory partition.</td>
</tr>
<tr>
<td>11.1.xx</td>
<td>SDX 14xxx, SDX 25xxx. <strong>Note:</strong> The clean-install option is supported on other SDX platforms if they have 10G factory partition</td>
</tr>
<tr>
<td>11.1.51.x</td>
<td>All the SDX platforms.</td>
</tr>
</tbody>
</table>

**Prerequisites**

Make sure that:
• You fail over all the primary HA nodes to a different SDX appliance. If you do not have HA capabilities, make sure that you plan for the downtime accordingly.
• Download the single bundle image to your local machine.

Important
Make sure that you do not restart or power cycle the appliance while using the Clean Install option.

To reset the Appliance to a single bundle image version:

1. Under Configuration tab, click System node and then under the System Administration group, click Appliance Reset.
2. In the Appliance Reset dialog box, select Clean Install in the Reset Type drop-down list, and click OK.

Cascading External Authentication Servers

January 23, 2019

Cascading multiple external authentication servers provides a continuous, reliable process for authenticating and authorizing external users. If authentication fails on the first authentication server, the Citrix NetScaler SDX Management Service attempts to authenticate the user by using the second external authentication server, and so on.

To enable cascading authentication, you need to add the external authentication servers to the Management Service. For more information, see Configuring External Authentication. You can add any type of the supported external authentication servers (RADIUS, LDAP, and TACACS). For example, if you want to add four external authentication servers for cascading authentication, you can add two RADIUS servers, one LDAP server, and one TACACS server, or four servers of the same type. You can configure up to 32 external authentication servers in Citrix Application Delivery Management.

To cascade external authentication servers:

1. On the Configuration tab, under System, expand Authentication.
2. In the Authentication page, click Authentication Configuration.
3. In the Authentication Configuration page, select EXTERNAL from the Server Type drop-down list (you can cascade only external servers).
4. Click Insert, and on the External Servers page that opens, select one or multiple authentication servers that you would like to cascade.
5. Click OK.

The selected servers are displayed on the Authentication Servers page as shown in the figure below.
You can specify the order of authentication by using the icon next to a server name to move the server up or down in the list.

**Provisioning Citrix NetScaler instances**

September 23, 2019

You can provision one or more Citrix NetScaler instances on the SDX appliance by using 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 Citrix NetScaler instances.

Provisioning a Citrix NetScaler VPX instance on the SDX appliance comprises the following steps.

1. Define an admin profile to attach to the Citrix NetScaler instance.
2. Upload the.xva image file to the Management Service.
3. Add a Citrix NetScaler instance using the Provision Citrix NetScaler wizard in Management Service. The Management Service implicitly deploys the Citrix NetScaler instance on the SDX appliance and then downloads configuration details of the instance.
Warning
To modify the provisioned network interfaces or VLANS of an instance, use the SDX Management Service GUI. Do not modify directly on the instance.

Create an admin profile

An admin profile specifies the user credentials that are used by the Management Service to:

- Provision the Citrix NetScaler instance
- Communicate with the instance to retrieve configuration data.

The user credentials specified in an admin profile are also used by the client when logging on to the Citrix NetScaler instances through the CLI or GUI.

By using the admin profile, you can specify that the Management Service and a VPX instance communicate with each other through a secure channel or HTTP.

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 must 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 Citrix NetScaler instance.

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

To change the password of Citrix NetScaler instances in a high-availability setup, use only the SDX GUI. Follow these steps:

1. Change the password on the instance designated as the secondary node.
2. Change the password on the instance designated as the primary node.

To create an admin profile

1. On the Configuration tab, in the navigation pane, expand Citrix NetScaler Configuration, and then click Admin Profiles.
2. In the Admin Profiles pane, click Add.
3. The Create Admin Profile dialog box appears.
Create Citrix ADC Profile

Profile Name*

User Name
nsroot

Password*

Use global settings for Citrix ADC communication

SNMP

Version
v2
v3

Security Name*

Security Level*
NoAuthNoPriv

Timeout Settings

commandcenter.timeout_settings

Timeout (in Seconds)
1800

Create  Close
Set the following parameters:

- **Profile Name**: name of the admin profile. The default profile name is nsroot. You can create user-defined profile names.
- **Password**: the password used to log on to the NetScaler instance. Maximum length: 31 characters.
- **SSH Port**: set the SSH port. The default port is 22.
- **Select Use global settings for NetScaler communication** check box. This option defines the setting in **System Settings** for communication between the Management Service and the NetScaler instance. You can clear this box and change the protocol to HTTP or HTTPS.
  - Select **http** option to use HTTP protocol for the communication between the Management Service and the Citrix NetScaler instance.
  - Select **https** option to use secure channel for the communication between the Management Service and the NetScaler instance.

1. Under **SNMP**, select the version. If you select v2, go to step 5. If you select v3, go to step 6.
2. Under SNMP v2, add the SNMP **Community** name.
3. Under SNMP v3, add **Security Name** and **Security Level**.
4. Under **Timeout Settings**, specify the value.
5. 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**.

**Upload a Citrix NetScaler.xva image**

A .xva file is required for adding a NetScaler VPX instance.

You have to upload the NetScaler C SDA .xva files to the SDX appliance before provisioning the VPX 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.
NetScaler SDX 11.1

- **Name**
  Name of the .xva image file. The file name contains the release version 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**.

**Add 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.
**Name**
Assign a name to the NetScaler instance.

Next, select an IPv4 or IPv6 address or both IPv4 and IPv6 addresses to access the Citrix VPX instance for management purpose.

A NetScaler instance can have only one management IP (also called NSIP). You cannot remove an NSIP address.

Assign a netmask, default gateway, and nexthop to Management Service for the IP address.
Next, add the XVA file, Admin Profile, and a description for the instance.

**Note:** For a high availability setup (active-active or active-standby), Citrix recommends that you configure the two NetScaler VPX 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.

### License allocation

In this section, specify the license you have procured for the NetScaler VPX appliance. The license can be Standard, Enterprise, and Platinum or Secure Web Gateway.

**Note:** * indicates required fields.
NetScaler SDX 11.1

Crypto allocation

Starting with release 11.1 57.11, the interface to manage crypto capacity has changed. For more information, see Manage crypto capacity

Resource allocation

Under resource allocation, assign total memory, packets per second, and CPU.

<table>
<thead>
<tr>
<th>Resource Allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Memory (MB)*</td>
</tr>
<tr>
<td>2048</td>
</tr>
<tr>
<td>Packets per second*</td>
</tr>
<tr>
<td>1000000</td>
</tr>
<tr>
<td>CPU*</td>
</tr>
<tr>
<td>Shared (1 core)</td>
</tr>
</tbody>
</table>

CPU

Assign a dedicated core or cores to the instance, or the instance shares a core with other instances. 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.

From SDX release 11.1.x.x (MR4), if you are using SDX 25000xx platform, you can assign a maximum of 16 cores to an instance. Also, if you are using SDX 2500xxx platform, you can assign a maximum of 11 cores to an instance.

Note: For an instance, the maximum throughput that you configure is 180 Gbps.

The following table lists the supported VPX, Single bungle image version, and the number of cores you can assign to an instance:
<table>
<thead>
<tr>
<th>Platform Name</th>
<th>Total Cores</th>
<th>Total Cores Available for VPX Provisioning</th>
<th>Maximum Cores That Can Be Assigned to a Single Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDX 8015, SDX 8400, and SDX 8600</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>SDX 8900</td>
<td>8</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500, and SDX 20500</td>
<td>12</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>SDX 11515, SDX 11520, SDX 11530, SDX 11540, and SDX 11542</td>
<td>12</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>SDX 17500, SDX 19500, and SDX 21500</td>
<td>12</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>SDX 17550, SDX 19550, SDX 20550, and SDX 21550</td>
<td>12</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 and SDX 14100</td>
<td>12</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>SDX 22040, SDX 22060, SDX 22080, SDX 22100, and SDX 22120</td>
<td>16</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>SDX 24100 and SDX 24150</td>
<td>16</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G and SDX 14100 40G</td>
<td>12</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>
## Instance administration

You can create an admin user for the VPX instance by selecting **Add Instance Administration** under **Instance Administration**.

<table>
<thead>
<tr>
<th>Platform Name</th>
<th>Total Cores</th>
<th>Total Cores Available for VPX Provisioning</th>
<th>Maximum Cores That Can Be Assigned to a Single Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS and SDX 14100. FIPS</td>
<td>12</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>SDX 14040 40S, SDX 14060 40S, SDX 14080 40S, and SDX 14100 40S</td>
<td>12</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>SDX 25100A, 25160A, 25200A</td>
<td>20</td>
<td>18</td>
<td>9</td>
</tr>
<tr>
<td>SDX 25100-40G, 25160-40G, 25200-40G</td>
<td>20</td>
<td>18</td>
<td>16 (if version is 11.1-51.x or higher); 9 (if version is 11.1-50.x or lower; all versions of 11.0 and 10.5)</td>
</tr>
<tr>
<td>SDX 26100, 26160, 26200, 26250</td>
<td>28</td>
<td>26</td>
<td>13</td>
</tr>
<tr>
<td>15000-50G</td>
<td>16</td>
<td>14</td>
<td>7</td>
</tr>
</tbody>
</table>
Add the following details:

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 user name.

Shell/Sftp/Scp Access: The access allowed to the NetScaler instance administrator. This option is selected by default.

**Network settings**

- Allow L2 Mode under network settings

You can allow L2 mode on the NetScaler instance. Select **Allow L2 Mode** under **Networking Settings**. 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.

By default interface 0/1 and 0/2 are selected for management LA.

VLAN tag: specify a VLAN ID for the management interface.

Next, add data interfaces.

Note: 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. This is because interface 1/4 is the first interface that you associated with instance 1.
• Allowed VLANs: Specify a list of VLAN IDs that can be associated with a NetScaler instance.

• MAC Address Mode: Assign a MAC address. Select from one of the following options:
  – Default: XenServer assigns a MAC address.
  – Custom: Choose this mode to specify a MAC address that overrides 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.

• VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)
- VRID IPV4: The IPv4 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.
- VRID IPV6: The IPv6 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.

Management VLAN settings

Typically, the Management Service and the management address (NSIP) of the 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 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 that you do not select NSVLAN. You cannot change this setting after you have provisioned the NetScaler instance.
**Note:**

- HA heartbeats are 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.

Click **Done** to provision the NetScaler VPX appliance.
Modify a NetScaler instance

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.

Restrict VLANs to specific virtual interfaces

The 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 one or more VLAN IDs 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 appliance 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 must be part of the VLAN.
6. Click Create, and then click Close.

Provisioning Third-Party Virtual Machines

January 23, 2019

The 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 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 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 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

January 23, 2019

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.

By using the Citrix 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 Citrix 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, see [SECUREMATRIX](#).

### Provisioning a SECUREMATRIX GSB Instance

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 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 SECUREM-TRIX 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**.

**Monitoring a SECUREMATRIX GSB Instance**

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.

Managing a SECUREMATRIX GSB 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 in:

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.

Upgrading the SDXTools File for a SECUREMATRIX GSB Instance

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.

**Upgrading and Downgrading SECUREMATRIX GSB Instance to a Later Version**

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.

**Troubleshooting a SECUREMATRIX GSB Instance**

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.

Trend Micro InterScan Web Security

January 23, 2019

Trend Micro 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 Citrix 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 an 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 have provisioned 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**

January 23, 2019

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.

**Provisioning a Websense Protector Instance**

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 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.

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.

**Monitoring a Websense Protector Instance**

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.

**Managing a Websense Protector 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.

**Upgrading the SDXTools File for a Websense Protector Instance**

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.

Upgrading the Websense Protector Instance to a Later Version

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.

Troubleshooting a Websense Protector Instance

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...
NetScaler SDX 11.1

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

January 23, 2019

BlueCat DNS/DHCP Server™ is a software solution that can be hosted on the Citrix 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 SDX to provide a smarter way to connect mobile devices, applications, virtual environments and clouds.

To learn more about BlueCat and Citrix, see https://citrixready.citrix.com/bluecat-networks.html.

If you are an existing BlueCat customer, you can download software and documentation via the BlueCat support portal at https://care.bluecatnetworks.com/.

© 1999-2020 Citrix Systems, Inc. All rights reserved.
Provisioning a BlueCat DNS/DHCP Instance

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 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.

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 Blue-
NetScaler SDX 11.1

Cat 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.

**Monitoring a BlueCat DNS/DHCP Instance**

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.

**Managing a BlueCat DNS/DHCP 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.

**Upgrading the SDXTools File for a BlueCat DNS/DHCP Instance**

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.

**Rediscovering a BlueCat DNS/DHCP Instance**

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**

April 2, 2020

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 documentation for that product.

### Provisioning a CA Access Gateway Instance

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 SDX appliance. Make sure you are using Management Service version 10.5 build 52.3.e or later on the 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.
Monitoring a CA Access Gateway Instance

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.

Managing a CA Access Gateway Instance

You can start, stop, restart, force stop, or force restart a CA Access Gateway instance from the Management Service. To complete these tasks, follow these steps:

1. On the Configuration tab, expand CA Access Gateway.
2. Navigate to CA Access Gateway > Instances.
3. 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
4. In the Confirm message box, click Yes.

Palo Alto Networks VM-Series

July 16, 2019

Note:
Provisioning Palo Alto VM-Series instances on a Citrix NetScaler SDX appliance is supported only on the SDX platforms 115XX, 84XX, 221XX, and 215XX.

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 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 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.

**Points to note:**

- The total number of instances that you can provision on an SDX appliance depends on the SDX hardware resources available.
- 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](https://www.paloaltonetworks.com/docs/

**Provisioning a Palo Alto VM-Series Instance**

Before you can provision a Palo Alto VM-Series instance, you must download an XVA image from the [Palo Alto Networks website](https://www.paloaltonetworks.com/). After you have downloaded the XVA image, upload it to the 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.

**Monitoring a Palo Alto VM-Series Instance**

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 Palo Alto VM-Series > Instances.
2. In the details pane, click the arrow next to the name of the instance.

### Managing a Palo Alto VM-Series Instance

You can start, stop, restart, force stop, or force restart a Palo Alto VM-Series instance from the Management Service.

On the **Configuration** tab, expand **Palo Alto VM-Series**.

1. Navigate to Palo Alto 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.

### Troubleshooting a Palo Alto VM-Series Instance

You can ping a Palo Alto 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 Palo Alto 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 **Palo Alto VM-Series**.

**To Ping an instance:**

1. Click **Instances**.
2. In the details pane, select the instance that you want to ping, and from the Action list, click Ping. The Ping message box shows whether the ping is successful.

**To Trace the route an instance:**

1. Click **Instances**.
2. In the details pane, select the instance that you want to ping, and from the Action list, click **TraceRoute**. The **Traceroute** message box displays the route to the instance.
To rediscover an instance:

1. Click **Instances**.
2. In the details pane, select the instance that you want to rediscover, and from the Action list, click **Rediscover**.
3. In the **Confirm** message box, click **Yes**.

Manage crypto capacity

May 30, 2019

Starting with release 11.1 57.11, 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 chip to ACU and 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.

**Table.** Unit crypto units

<table>
<thead>
<tr>
<th>New crypto units</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asymmetric crypto unit (ACU)</td>
<td>1 ACU = 1 operation per second (ops) of (RSA) 2 K (2048-bit key size) decryption. For further details, see ACU to PKE resource conversion table.</td>
</tr>
<tr>
<td>Symmetric crypto unit (SCU)</td>
<td>1 SCU = 1 Mbps of AES-128-CBC + SHA256-HMAC @ 1024B. This definition is applicable for all SDX platforms.</td>
</tr>
</tbody>
</table>
View crypto capacity of the SDX appliance

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, under Crypto Allocation, 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, follow these steps.

1. Log on to the Management Service.
2. Navigate to Configuration > NetScaler > Instances, and click Add.
3. Under **Crypto Allocation**, 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 specified number.

### Minimum value of an ACU counter available for different SDX appliances table

<table>
<thead>
<tr>
<th>NetScaler SDX platform</th>
<th>ACU counter minimum value</th>
</tr>
</thead>
<tbody>
<tr>
<td>22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ports)</td>
<td>2187</td>
</tr>
<tr>
<td>8400, 8600, 8010, 8015</td>
<td>2812</td>
</tr>
<tr>
<td>17500, 19500, 21500</td>
<td>2812</td>
</tr>
<tr>
<td>17550, 19550, 20550, 21550</td>
<td>2812</td>
</tr>
<tr>
<td>11500, 13500, 14500, 16500, 18500, 20500</td>
<td>2812</td>
</tr>
<tr>
<td>11515, 11520, 11530, 11540, 11542</td>
<td>4375</td>
</tr>
<tr>
<td>14xxx</td>
<td>4375</td>
</tr>
<tr>
<td>14xxx 40S</td>
<td>4375</td>
</tr>
<tr>
<td>14xxx 40G</td>
<td>4375</td>
</tr>
<tr>
<td>14xxx FIPS</td>
<td>4375</td>
</tr>
<tr>
<td>25xxx</td>
<td>4375</td>
</tr>
<tr>
<td>25xxx A</td>
<td>4575</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Crypto Allocation</th>
<th>Asymmetric Crypto Units</th>
<th>Symmetric Crypto Units</th>
<th>Crypto Virtual Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>30000</td>
<td>40000</td>
<td>32</td>
</tr>
<tr>
<td>Total</td>
<td>30000</td>
<td>40000</td>
<td>32</td>
</tr>
</tbody>
</table>

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

**View crypto hardware health**

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 11.1 57.11 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.

ACU to PKE resource conversion table

<table>
<thead>
<tr>
<th>NetScaler SDX platform</th>
<th>ACU</th>
<th>RSA-RSA1K</th>
<th>RSA-RSA2K</th>
<th>RSA-RSA4K</th>
<th>ECDHE-RSA</th>
<th>ECDHE-ECDSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ports)</td>
<td>2187</td>
<td>12497</td>
<td>2187</td>
<td>312</td>
<td>256</td>
<td>190</td>
</tr>
<tr>
<td>8400, 8600, 8010, 8015</td>
<td>2812</td>
<td>17000</td>
<td>2812</td>
<td>424</td>
<td>330</td>
<td>N/A</td>
</tr>
<tr>
<td>11515, 11520, 11530, 11540, 11542</td>
<td>4375</td>
<td>25000</td>
<td>4375</td>
<td>625</td>
<td>512</td>
<td>381</td>
</tr>
<tr>
<td>22040, 22060, 22080, 22100, 22120 (24 ports)</td>
<td>4375</td>
<td>25000</td>
<td>4375</td>
<td>625</td>
<td>512</td>
<td>381</td>
</tr>
</tbody>
</table>
### NetScaler SDX 11.1

**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.

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

<table>
<thead>
<tr>
<th>NetScaler SDX platform</th>
<th>ACU</th>
<th>RSA-RSA1K</th>
<th>RSA-RSA2K</th>
<th>RSA-RSA4K</th>
<th>ECDHE-RSA</th>
<th>ECDHE-ECDSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>17500, 19500, 21500</td>
<td>2812</td>
<td>17000</td>
<td>2812</td>
<td>424</td>
<td>330</td>
<td>N/A</td>
</tr>
<tr>
<td>17550, 19550, 20550, 21550</td>
<td>2812</td>
<td>17000</td>
<td>2812</td>
<td>424</td>
<td>330</td>
<td>N/A</td>
</tr>
<tr>
<td>11500, 13500, 14500, 16500, 18500, 20500</td>
<td>2812</td>
<td>17000</td>
<td>2812</td>
<td>424</td>
<td>330</td>
<td>N/A</td>
</tr>
<tr>
<td>14xxx, 14xxx, 40G, 25xxx, 25xxx A</td>
<td>4375</td>
<td>25000</td>
<td>4375</td>
<td>625</td>
<td>512</td>
<td>381</td>
</tr>
<tr>
<td>14xxx FIPS</td>
<td>4375</td>
<td>25000</td>
<td>4375</td>
<td>625</td>
<td>512</td>
<td>381</td>
</tr>
<tr>
<td>14xxx 40S</td>
<td>4375</td>
<td>25000</td>
<td>4375</td>
<td>625</td>
<td>512</td>
<td>381</td>
</tr>
<tr>
<td>*89xx</td>
<td>1000</td>
<td>4615</td>
<td>1000</td>
<td>136</td>
<td>397</td>
<td>4949</td>
</tr>
<tr>
<td>*26xxx</td>
<td>1000</td>
<td>4615</td>
<td>1000</td>
<td>136</td>
<td>397</td>
<td>4949</td>
</tr>
<tr>
<td>*15000 50G</td>
<td>1000</td>
<td>4615</td>
<td>1000</td>
<td>136</td>
<td>397</td>
<td>4949</td>
</tr>
</tbody>
</table>

© 1999-2020 Citrix Systems, Inc. All rights reserved.
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.

**Legacy SSL chips to ACU and SCU conversion table**

For more information about how legacy SSL chips are converted to ACU and SCU, see the following table.

**ACU and SCU conversion table**

**Bandwidth Metering in SDX**

June 25, 2019

Citrix NetScaler 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**

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

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 Throughput 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,
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:

---

Configuring and Managing Citrix NetScaler instances

January 23, 2019

After you have provisioned Citrix NetScaler instances on your appliance, you are ready to configure and manage the instances. Begin by creating a subnet IP (SNIP) 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 SNIP Address on a Citrix NetScaler instance

You can assign a SNIP address to the Citrix NetScaler instances after it is 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 Citrix NetScaler SDX appliance. You can assign SNIP to the Citrix NetScaler instance from the Management Service.

To add a SNIP Address on a Citrix 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 address.
   - Netmask: specify the subnet mask associated with the SNIP address.
   - Type: By default the value is SNIP.
   - Save Configuration: Specify whether the configuration should be saved on the Citrix NetScaler. Default value is false.
   - Instance IPAddress: Specify the IP address of the Citrix NetScaler instance.
4. Click Create, and then click Close.

Saving the Configuration

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

To save the configuration on a Citrix 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 IPAddress, select the IP addresses of the Citrix NetScaler instances whose configuration you want to save.
4. Click OK, and then click Close.

Managing a Citrix NetScaler instance

The Management Service lets you perform the following operations on the Citrix NetScaler instances, both from the Citrix NetScaler instances pane in the Configuration tab and in the Citrix NetScaler instances gadget on the Home page.
**Start a Citrix NetScaler instance:**
Start any Citrix NetScaler instance from the Management Service user interface. When the Management Service UI forwards this request to the Management Service, it starts the Citrix NetScaler instance.

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

**Reboot a Citrix NetScaler instance:**
Restart the Citrix NetScaler instance.

**Delete a Citrix NetScaler instance:**
If you do not want to use a Citrix 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 Citrix NetScaler instance**
1. On the Configuration tab, in the navigation pane, click Citrix NetScaler instances.
2. In the Citrix NetScaler instances pane, select the Citrix 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 Citrix NetScaler instance Files**
You can remove any Citrix NetScaler instance files, such as XVAs, builds, documentation, SSL keys or SSL certificates, from the appliance.

**To remove Citrix 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 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 VPX instance are on different subnetworks and the router is down or if the Management Service and VPX instance are on the same subnets 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 VPX instance at any time.

To apply the admin configuration on a Citrix 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 IPAddress, select the IP address of the VPX instance on which you want to apply the admin configuration.
4. Click OK.

Monitoring Citrix NetScaler instances

January 23, 2019

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

Viewing the properties of VPX instances

The Management Service user interface displays the list and description of all the VPX instances provisioned on the SDX appliance. Use the Citrix 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 VPX instance opens the configuration utility (GUI) of that instance in a new tab or browser.
To view the properties of 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 VPX instance from the Home tab.

2. In the Citrix NetScaler instance pane, you can view the following details for the Citrix NetScaler instance:
   - Name
     The hostname assigned to the Citrix NetScaler instance while provisioning.
   - VM State
     The state of the virtual machine.
   - NetScaler State
     The state of the Citrix NetScaler instance.
   - IP Address
     The IP address of the Citrix 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 Citrix NetScaler instance.
   - Tx (Mbps)
     The packets transmitted by the Citrix NetScaler instance.
   - HTTP Req/s
     The total number of HTTP requests received on the Citrix NetScaler instance every second.
   - CPU Usage (%)
     The percentage of CPU utilization on the Citrix NetScaler.
   - Memory Usage (%)
     The percentage of memory utilization on the Citrix NetScaler.

3. Click the arrow next to the name of a Citrix NetScaler instance to view the properties of that instance, or click Expand All to view the properties of all the Citrix NetScaler instances. You can view the following properties:
   - Netmask
     The netmask IP address of the Citrix 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 Citrix NetScaler instance, along with the virtual function assigned to each interface.

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

• Host Name
  The host name of the Citrix NetScaler instance.

• Total Memory (GB)
  The total memory being assigned to the Citrix NetScaler instance.

• Throughput (Mbps)
  The total throughput of the Citrix 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 Citrix NetScaler instance if it is in an HA setup.

• Status
  The status of the operations being performed on a Citrix 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 Citrix NetScaler instance.

Viewing the Running and Saved Configuration of a Citrix NetScaler instance

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

To view the running and saved configuration of a Citrix NetScaler instance

1. On the Configuration tab, in the left pane, expand NetScaler Configuration, and then click Instances.
2. In the Citrix NetScaler instances pane, click the Citrix 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 Citrix NetScaler instance.

Pinging a Citrix NetScaler instance

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

To ping a Citrix NetScaler instance

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

Tracing the Route of a Citrix NetScaler instance

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

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

Rediscovering a Citrix NetScaler instance

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

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

January 23, 2019

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

Viewing the audit logs

All operations performed by using the Management Service are logged in the appliance database. Use audit logs to view the operations that a Management Service user has performed, the date and time of each operation, and the success or failure status of the operation. You can also sort the details by user, operation, audit time, status, and so on by clicking the appropriate column heading.
Pagination is supported in the Audit Log pane. Select the number of records to display on a page. By default, 25 records are displayed on a page.

To view audit logs, follow these steps:

1. In the navigation pane, expand System, and then click Audit.
2. In the Audit Log pane, you can view the following details.
   - User Name: the Management Service user who has performed the operation.
   - IP Address: the IP address of the system on which the operation was performed.
   - Port: the port at which the system was running when the operation was performed.
   - Resource Type: the type of resource used to perform the operation, such as xen_vpx_image and login.
   - Resource Name: the name of the resource used to perform the operation, such as vpx_image_name and the user name used to log in.
   - Audit Time: the time when the audit log was generated.
   - Operation: the task that was performed, such as add, delete, and log out.
   - Status: the status of the audit, such as Success or Failed.
   - Message: a message describing the cause of failure if the operation has failed and status of the task, such as Done, if the operation was successful.
3. To sort the logs by a particular field, click the heading of the column.

**Viewing Task Logs**

Use task logs to view and track tasks, such as upgrading instances and installing SSL certificates, that are executed by the Management Service on the Citrix 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, follow these steps:

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.
Viewing Task Device Logs

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

To view the task device log, follow these steps:

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 Citrix NetScaler instance. The task command log lets you view whether a command has been successfully executed or has failed. It also displays the command that is executed and the reason why a command has failed.

To view the task command log, follow these steps:

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

Viewing Events

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

To view the events, follow these steps:

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 Citrix ADC SDX Appliances

January 23, 2019

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 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 Citrix 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 Citrix NetScaler instances are in the same network.
- Consolidation when the Management Service and the Citrix NetScaler instances are in different networks but all the instances are in the same network.
- Consolidation across security.
- 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 Citrix ADC instances are in the Same Network

January 23, 2019

A simple type of consolidation case on the SDX appliance is configuration of the Management Service and the Citrix ADC 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 Citrix ADC 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 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 NSIPs for instances in the same network

The following table lists the names and values of the parameters used for provisioning Citrix ADC instance 1 in the above example.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Values for Instance 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vpx8</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.1.2</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>XVA File</td>
<td>NS-VPX-XEN-10.0-51.308.a_nc.xva</td>
</tr>
<tr>
<td>Feature License</td>
<td>Platinum</td>
</tr>
<tr>
<td>Admin Profile</td>
<td>ns_nsroot_profile</td>
</tr>
<tr>
<td>User Name</td>
<td>vpx8</td>
</tr>
</tbody>
</table>
## Provision Citrix ADC instance 1 as shown in this example

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the Citrix ADC 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 Citrix ADC instance you provisioned appears in the Citrix ADC instances pane.

## Consolidation When the Management Service and the Citrix NetScaler instances are in Different Networks

June 25, 2019

In certain cases, the appliance administrator might allow other administrators to perform administrative 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 Citrix 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 Add a Citrix NetScaler instance section in Provisioning Citrix NetScaler instances.

The following figure illustrates the above use case.

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 Citrix NetScaler instance 1 in this example.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Values for Instance 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vpx1</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.2.2</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>10.1.2.1</td>
</tr>
<tr>
<td>XVA File</td>
<td>NS-VPX-XEN-10.0-51.308.a_nc.xva</td>
</tr>
<tr>
<td>Feature License</td>
<td>Platinum</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Values for Instance 1</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Admin Profile</td>
<td>ns_nsroot_profile</td>
</tr>
<tr>
<td>User Name</td>
<td>vpx1</td>
</tr>
<tr>
<td>Password</td>
<td>Sdx</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Sdx</td>
</tr>
<tr>
<td>Shell/Sftp/Scp Access</td>
<td>True</td>
</tr>
<tr>
<td>Total Memory (MB)</td>
<td>2048</td>
</tr>
<tr>
<td>#SSL Chips</td>
<td>1</td>
</tr>
<tr>
<td>Throughput (Mbps)</td>
<td>1000</td>
</tr>
<tr>
<td>Packets per second</td>
<td>10000000</td>
</tr>
<tr>
<td>CPU</td>
<td>Shared</td>
</tr>
<tr>
<td>Interface</td>
<td>0/2 and 1/1</td>
</tr>
</tbody>
</table>

To provision Citrix NetScaler instance 1 as shown in this example

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the Citrix 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 Citrix NetScaler instance you provisioned appears in the Citrix NetScaler instances pane.

Consolidation Across Security Zones

January 23, 2019

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 Citrix ADC 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 Citrix ADC 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

January 23, 2019

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. Citrix NetScaler instances 2 and 3 are part of the 10.1.200.x network (VLAN 100), and Citrix 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 Citrix 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 Citrix NetScaler instances 5 and 3 in this example.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Values for Instance 5</th>
<th>Values for Instance 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vpx5</td>
<td>vpx3</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.3.2</td>
<td>10.1.200.2</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td>255.255.255.240</td>
</tr>
<tr>
<td>Gateway</td>
<td>10.1.3.1</td>
<td>10.1.200.1</td>
</tr>
<tr>
<td>XVA File</td>
<td>NS-VPX-XEN-10.0-51.308.a_nc.xva</td>
<td>NS-VPX-XEN-10.0-51.308.a_nc.xva</td>
</tr>
<tr>
<td>Feature License</td>
<td>Platinum</td>
<td>Platinum</td>
</tr>
<tr>
<td>Admin Profile</td>
<td>ns_nsroot_profile</td>
<td>ns_nsroot_profile</td>
</tr>
<tr>
<td>User Name</td>
<td>vpx5</td>
<td>vpx3</td>
</tr>
<tr>
<td>Password</td>
<td>Sdx</td>
<td>root</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Sdx</td>
<td>root</td>
</tr>
<tr>
<td>Shell/Sftp/Scp Access</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Total Memory (MB)</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td>#SSL Chips</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Throughput (Mbps)</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Packets per second</td>
<td>1000000</td>
<td>1000000</td>
</tr>
<tr>
<td>CPU</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>Interface</td>
<td>1/1 and 10/4</td>
<td>1/1 and 1/5</td>
</tr>
<tr>
<td>NSVLAN</td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td>Add (interface)</td>
<td>1/1</td>
<td>1/1</td>
</tr>
<tr>
<td>Tagged Interface</td>
<td>Select Tagged</td>
<td>Select Tagged</td>
</tr>
</tbody>
</table>

To provision Citrix NetScaler instances 5 and 3 as shown in this example

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the Citrix 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 Citrix NetScaler instance you provisioned appears in the Citrix NetScaler instances pane.

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

January 23, 2019

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.
- Citrix 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 Citrix NetScaler instances distributed across networks

© 1999-2020 Citrix Systems, Inc. All rights reserved.
The following table lists the names and values of the parameters used for provisioning Citrix NetScaler instances 7 and 4 in this example.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Values for Instance 7</th>
<th>Values for Instance 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>vpx7</td>
<td>vpx4</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.3.7</td>
<td>10.1.3.4</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td>255.255.255.240</td>
</tr>
<tr>
<td>Gateway</td>
<td>10.1.3.1</td>
<td>10.1.3.1</td>
</tr>
<tr>
<td>XVA File</td>
<td>NS-VPX-XEN-10.0-51.308.a_nc.xva</td>
<td>NS-VPX-XEN-10.0-51.308.a_nc.xva</td>
</tr>
<tr>
<td>Feature License</td>
<td>Platinum</td>
<td>Platinum</td>
</tr>
<tr>
<td>Admin Profile</td>
<td>ns_nsroot_profile</td>
<td>ns_nsroot_profile</td>
</tr>
<tr>
<td>User Name</td>
<td>vpx4</td>
<td>vpx4</td>
</tr>
<tr>
<td>Password</td>
<td>Sdx</td>
<td>Sdx</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Sdx</td>
<td>Sdx</td>
</tr>
<tr>
<td>Shell/Sftp/Scp Access</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Total Memory (MB)</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td>#SSL Chips</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Throughput (Mbps)</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>Packets per second</td>
<td>1000000</td>
<td>1000000</td>
</tr>
<tr>
<td>CPU</td>
<td>Shared</td>
<td>Shared</td>
</tr>
<tr>
<td>Interface</td>
<td>1/1 and 1/7</td>
<td>1/1 and 1/7</td>
</tr>
<tr>
<td>NSVLAN</td>
<td>200</td>
<td>200</td>
</tr>
</tbody>
</table>
**To provision Citrix NetScaler instances 7 and 4 in this example**

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the Citrix 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 Citrix NetScaler instance you provisioned appears in the Citrix NetScaler instances pane.

---

**NITRO API**

January 23, 2019

The Citrix SDX NITRO protocol allows you to configure and monitor the 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 SDX appliance before using NITRO.

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

- Access to a SDX appliance.
- To use REST interfaces, you must have a system to generate HTTP or HTTPS requests (payload in JSON format) to the 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](http://www.oracle.com/technetwork/java/javase/downloads/index.html).
- 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**

June 19, 2019
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.

.NET SDK

June 19, 2019

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:

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

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:

1 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:

1 ns newns = new ns();
2
3 //Set the properties of the NetScaler locally
4 newns.name = "ns_instance";
5 newns.ip_address = "10.70.136.5";
6 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];

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

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:

```
pre codeblock
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.
   
   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:

```javascript
nsobj = new ns();
obj.id = "123456a";
n.s.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:

```javascript
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**

June 19, 2019

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

Each resource also has a state on which the following operations can be performed:
• **Create.** Clients can create new server-side resources on a “container” resource. You can think of container resources as folders, and child resources as files or subfolders. The calling client provides the state for the resource to be created. The state can be specified in the request by using XML or JSON format. The client can also specify the unique URL that will identify the new object. Alternatively, the server can choose and return a unique URL identifying the created object. The HTTP method used for create requests is POST.

• **Read.** Clients can retrieve the state of a resource by specifying its URL with the HTTP GET method. The response message contains the resource state, expressed in JSON format.

• **Update.** You can update the state of an existing resource by specifying the URL that identifies that object and its new state in JSON or XML, using the PUT HTTP method.

• **Delete.** You can destroy a resource that exists on the server-side by using the DELETE HTTP method and the URL identifying the resource to be removed.

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

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

**System APIs**

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

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

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

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

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

```plaintext
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’.

© 1999-2020 Citrix Systems, Inc. All rights reserved.
- **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**
NetScaler SDX 11.1

- **Payload**

```json
{
    "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**

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
NetScaler SDX 11.1

a NetScaler instance named vpx1:

- **URL.** [https://10.102.31.16/nitro/v2/config/ns/](https://10.102.31.16/nitro/v2/config/ns/)
- **HTTP Method.** POST
- **Request.**
  - **Header**
    ```
    1  Cookie:NITRO_AUTH_TOKEN=tokenvalue
    2  Content-Type:application/vnd.com.citrix.sdx.ns+json
    ```
  - **Payload**
    ```
    1  {
    2  "ns":
    3  {
    4  "name": "vpx1",
    5  "ip_address": "192.168.100.2",
    6  "netmask": "255.255.255.0",
    7  "gateway": "192.168.100.1",
    8  "image_name": "nsvpx-9.3-45_nc.xva",
    9  "vm_memory_total": 2048,
    10  "throughput": 1000,
    11  "pps": 1000000,
    12  "license": "Standard",
    13  "profile_name": "ns_nsroot_profile",
    14  "username": "admin",
    15  "password": "admin",
    16  "network_interfaces":
    17  [
    18  {
    19  "port_name": "10/1"
    20  },
    21  {
    22  "port_name": "10/2"
    23  }
    24  ]
    25  }
    26  }
    ```
NetScaler SDX 11.1

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: \texttt{http://\langle IP\rangle/nitro/v2/config/\langle resource\_type\rangle?filter=\langle property1\rangle::\langle value\rangle,\langle property2\rangle::\langle value\rangle}.

- 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: \texttt{http://\langle IP\rangle/nitro/v2/config/\langle resource\_type\rangle?pageno=\langle value\rangle\&pagesize=\langle value\rangle}.

  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 \texttt{http://\langle IP\rangle/nitro/v2/config/\langle resource\_type\rangle?count=yes}.

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

- **URL.** \texttt{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:
NetScaler SDX 11.1

• **URL.** https://10.102.31.16/nitro/v2/config/ns/
• **HTTP Method.**
• **Request Payload.**
  – **Header**

```plaintext
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sd.x.ns+json
```

– **Payload**

```plaintext
1 {
2   "ns": {
3     "name": "vpx2",
4       "id": "123456a"
5   }
6 }
```

**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**

```plaintext
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sd.x.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.**
  
  ```
  {  
    "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.

How NITRO works

June 19, 2019

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

June 19, 2019

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:

```java
//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");
```
NetScaler SDX 11.1

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:

```
1 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:

```
1 ns newns = new ns();
2
3 //Set the properties of the NetScaler locally
4 newns.set_name("ns_instance");
5 newns.set_ip_address("10.70.136.5");
6 newns.set_netmask("255.255.255.0");
7 newns.set_gateway("10.70.136.1");
8 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:

```java
//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:

```java
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':

```java
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:

```java
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:

```java
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.

**SDX Command Reference**

September 23, 2019

For the detailed list of the commands that can be used to configure the Citrix NetScaler SDX appliance through the CLI, see SDX 11.1 doc set.