



Citrix NetScaler SDX Administration Guide

Copyright and Trademark Notice

© CITRIX SYSTEMS, INC., 2012. ALL RIGHTS RESERVED. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS OR USED TO MAKE DERIVATIVE WORK (SUCH AS TRANSLATION, TRANSFORMATION, OR ADAPTATION) WITHOUT THE EXPRESS WRITTEN PERMISSION OF CITRIX SYSTEMS, INC.

ALTHOUGH THE MATERIAL PRESENTED IN THIS DOCUMENT IS BELIEVED TO BE ACCURATE, IT IS PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE ALL RESPONSIBILITY FOR THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS MANUAL.

CITRIX SYSTEMS, INC. OR ITS SUPPLIERS DO NOT ASSUME ANY LIABILITY THAT MAY OCCUR DUE TO THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS DOCUMENT. INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. COMPANIES, NAMES, AND DATA USED IN EXAMPLES ARE FICTITIOUS UNLESS OTHERWISE NOTED.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Citrix' written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler appliance. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

Move the NetScaler equipment to one side or the other of your equipment.

Move the NetScaler equipment farther away from your equipment.

Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Citrix Systems, Inc., could void the FCC approval and negate your authority to operate the product.

BroadCom is a registered trademark of BroadCom Corporation. Fast Ramp, NetScaler, and NetScaler Request Switch are trademarks of Citrix Systems, Inc. Linux is a registered trademark of Linus Torvalds. Internet Explorer, Microsoft, PowerPoint, Windows and Windows product names such as Windows NT are trademarks or registered trademarks of the Microsoft Corporation. NetScape is a registered trademark of Netscape Communications Corporation. Red Hat is a trademark of Red Hat, Inc. Sun and Sun Microsystems are registered trademarks of Sun Microsystems, Inc. Other brand and product names may be registered trademarks or trademarks of their respective holders.

Software covered by the following third party copyrights may be included with this product and will also be subject to the software license agreement: Copyright 1998 © Carnegie Mellon University. All rights reserved. Copyright © David L. Mills 1993, 1994. Copyright © 1992, 1993, 1994, 1997 Henry Spencer. Copyright © Jean-loup Gailly and Mark Adler. Copyright © 1999, 2000 by Jef Poskanzer. All rights reserved. Copyright © Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, Kevin Steves. All rights reserved. Copyright © 1982, 1985, 1986, 1988-1991, 1993 Regents of the University of California. All rights reserved. Copyright © 1995 Tatu Ylonen, Espoo, Finland. All rights reserved. Copyright © UNIX System Laboratories, Inc. Copyright © 2001 Mark R V Murray. Copyright 1995-1998 © Eric Young. Copyright © 1995, 1996, 1997, 1998. Lars Fenneberg. Copyright © 1992. Livingston Enterprises, Inc. Copyright © 1992, 1993, 1994, 1995. The Regents of the University of Michigan and Merit Network, Inc. Copyright © 1991-2, RSA Data Security, Inc. Created 1991. Copyright © 1998 Juniper Networks, Inc. All rights reserved. Copyright © 2001, 2002 Networks Associates Technology, Inc. All rights reserved. Copyright (c) 2002 Networks Associates Technology, Inc. Copyright 1999-2001 © The Open LDAP Foundation. All Rights Reserved. Copyright © 1999 Andrzej Bialecki. All rights reserved. Copyright © 2000 The Apache Software Foundation. All rights reserved. Copyright (C) 2001-2003 Robert A. van Engelen, Genivia inc. All Rights Reserved. Copyright (c) 1997-2004 University of Cambridge. All rights reserved. Copyright (c) 1995. David Greenman. Copyright (c) 2001 Jonathan Lemon. All rights reserved. Copyright (c) 1997, 1998, 1999. Bill Paul. All rights reserved. Copyright (c) 1994-1997 Matt Thomas.

All rights reserved. Copyright © 2000 Jason L. Wright. Copyright © 2000 Theo de Raadt. Copyright © 2001 Patrik Lindergrén.

All rights reserved.

Last Updated: July 2012

Document code: July 26 2012 03:36:30

Contents

Preface.....	11
Formatting Conventions for NetScaler Documentation	11
Documentation Available on the NetScaler Appliance	12
Getting Service and Support	13
NetScaler Documentation Feedback	13
 1 Introduction.....	15
Getting Started with the Management Service User Interface.....	16
Logging on to the Management Service User Interface.....	16
To log on to the Management Service user interface.....	16
Provisioning NetScaler Instances.....	17
Single Sign-On to the Management Service and the NetScaler Instances.....	17
To log on to a NetScaler instance from the Management Service.....	17
Managing the Home Page.....	17
 2 Managing and Monitoring the NetScaler SDX Appliance.....	19
Modifying the Network Configuration of the SDX Appliance.....	20
To modify the network configuration of the SDX appliance.....	20
Changing the Password of the Default User Account.....	20
To change the password of the default user account.....	21
Configuring Clock Synchronization.....	21
To configure an NTP server.....	21
To enable NTP synchronization	22
To modify Authentication options	22
SNMP.....	23
SNMP Trap Destinations	23
To add an SNMP trap destination	24
Downloading MIB Files	24
To download MIB files.....	24
Managing Licenses.....	25
To upload a license file to the SDX appliance.....	25
To apply the licenses that have been uploaded to the SDX appliance.....	25

To create a backup by downloading a license file.....	26
Managing Interfaces.....	26
To configure an interface.....	26
To reset the parameters of an interface to their default values.....	27
VLAN Filtering.....	27
To enable VLAN filtering on an interface.....	28
Viewing the SSL Certificate on the Management Service.....	28
To view the SSL certificate on the Management Service.....	28
Viewing the Properties of the NetScaler SDX Appliance.....	28
Viewing Real-Time Appliance Throughput.....	30
Viewing Real-Time CPU and Memory Usage.....	30
Viewing CPU Usage for All Cores.....	30
Restarting the Appliance.....	31
To restart the appliance.....	31
Shutting Down the Appliance.....	31
To shut down the appliance.....	31
Modifying the Time Zone on the Appliance.....	31
To modify the time zone on the appliance.....	31
Modifying System Settings.....	31
To modify system settings.....	32
System Health Monitoring.....	32
Monitoring the Resources on the SDX Appliance.....	32
Monitoring the Storage Resources on the SDX Appliance.....	33
Monitoring the Hardware Sensors on the SDX Appliance.....	34
Monitoring the Interfaces on the SDX Appliance.....	35
3 Configuring the Management Service.....	37
Managing Client Sessions.....	38
Configuring User Accounts.....	38
To configure a user account.....	38
To remove a user account.....	39
Configuring Policies.....	39
To specify the number of days for which logged data is pruned.....	40
To specify the number of backups that the appliance must retain.....	40
SNMP Trap Destinations.....	40
To add a trap destination.....	40
Restarting the Management Service.....	41
To restart the Management Service.....	41
Upgrading the Management Service.....	41

Uploading the Management Service Build and Documentation Files.....	42
To upload the Management Service build file.....	42
To create a backup by downloading a Management Service build file.....	42
To upload the Management Service documentation file.....	42
To create a backup by downloading a Management Service documentation file.....	42
Upgrading the Management Service to a Later Version.....	43
To upgrade the Management Service.....	43
Upgrading the XenServer Software.....	43
Uploading the XenServer Build Files.....	43
To upload the XenServer build file.....	43
To create a backup by downloading a XenServer build file.....	44
Upgrading the XenServer Software to a Later Version.....	44
To upgrade the XenServer software.....	44
Backing Up and Restoring the Configuration Data of the SDX Appliance.....	44
To perform an immediate backup.....	44
To restore the configuration.....	45
Performing a Factory Reset.....	45
To perform a factory reset.....	46
Removing Management Service Files.....	46
To remove a Management Service file.....	46
Generating a Tar Archive for Technical Support.....	46
To generate the tar archive for technical support.....	47
To download the tar archive for technical support.....	47
 4 Provisioning NetScaler Instances.....	49
Creating Admin Profiles.....	50
To create an admin profile.....	50
Uploading NetScaler .Xva Images.....	51
To upload a NetScaler .xva file.....	51
To create a backup by downloading a NetScaler .xva file.....	51
Adding a NetScaler Instance.....	52
To provision a NetScaler instance.....	54
 5 Configuring and Managing NetScaler Instances	57
Creating a Mapped IP Address or a Subnet IP Address on a NetScaler Instance.....	58
To add a MIP or SNIP on a NetScaler instance.....	58
Saving the Configuration.....	58
To save the configuration on a NetScaler instance.....	59

Installing SSL Certificates.....	59
Uploading the Certificate File to the SDX Appliance.....	59
To upload SSL certificate files to the SDX appliance.....	59
To create a backup by downloading an SSL certificate file.....	59
Uploading SSL Key Files to the SDX Appliance.....	60
To upload SSL key files to the SDX appliance.....	60
To create a backup by downloading an SSL key file.....	60
Installing an SSL Certificate on a NetScaler Instance.....	60
To install SSL certificates on a NetScaler instance.....	61
Upgrading a NetScaler Instance.....	61
Uploading the NetScaler Software Images, Documentation, and XVA Files and Documentation Files.....	62
To upload a NetScaler software image.....	62
To create a backup by downloading a NetScaler build file.....	62
To upload a NetScaler documentation file.....	62
To create a backup by downloading a NetScaler documentation file.....	63
To upload a NetScaler XVA file.....	63
To create a backup by downloading a NetScaler XVA file.....	63
Upgrading Multiple NetScaler VPX Instances.....	63
To upgrade a NetScaler VPX instance image.....	64
Managing a NetScaler Instance.....	64
To start, stop, delete, or restart a NetScaler instance.....	64
Removing NetScaler Instance Files.....	65
To remove NetScaler instance files.....	65
Applying the Administration Configuration.....	65
To apply the admin configuration on a NetScaler instance.....	65
6 Monitoring NetScaler Instances.....	67
Viewing the Properties of the NetScaler Instance.....	68
To view the properties of NetScaler VPX instances.....	68
Viewing the Running and Saved Configuration of a NetScaler Instance.....	70
To view the running and saved configuration of a NetScaler instance.....	70
Pinging a NetScaler Instance.....	70
To ping a NetScaler instance.....	70
Tracing the Route of a NetScaler Instance.....	70
To trace the route of a NetScaler instance.....	71
Rediscovering a NetScaler Instance.....	71
To rediscover a NetScaler instance.....	71

7	Using Logs to Monitor Operations and Events.....	73
	Viewing Audit Logs.....	74
	To view audit logs.....	74
	Viewing Task Logs.....	75
	To view the task log.....	75
	Viewing Task Device Logs.....	75
	To view the task device log.....	75
	Viewing Task Command Logs.....	76
	To view the task command log.....	76
	Viewing Events.....	76
	To view the events.....	76
8	Use Cases for NetScaler SDX Appliance.....	77
	Consolidation When the Management Service and the NetScaler Instances are in the Same Network.....	78
	To provision NetScaler Instance 1 as shown in this example.....	79
	Consolidation When the Management Service and the NetScaler Instances are in Different Networks.....	80
	To provision NetScaler Instance 1 as shown in this example.....	82
	Consolidation Across Security Zones.....	82
	Consolidation with Dedicated Interfaces for Each Instance.....	83
	To provision NetScaler Instances 5 and 3 as shown in this example.....	84
	Consolidation With Sharing of a Physical Port by More Than One Instance.....	85
	To provision NetScaler Instances 7 and 4 in this example.....	87

Preface

Learn about the Citrix® NetScaler® collection of documentation, including information about support options and ways to send us feedback.

In This Preface:

- ♦ Formatting Conventions for NetScaler Documentation
- ♦ Documentation Available on the NetScaler Appliance
- ♦ Getting Service and Support
- ♦ NetScaler Documentation Feedback

For information about new features and enhancements for this release, see the *Citrix NetScaler 9.3 Release Notes* at <http://support.citrix.com/article/CTX128669>.

Formatting Conventions for NetScaler Documentation

The NetScaler documentation uses the following formatting conventions.

Table 1. Formatting Conventions

Convention	Meaning
Boldface	In text paragraphs or steps in a procedure, information that you type exactly as shown (user input), or an element in the user interface.
<code>Monospace</code>	Text that appears in a command-line interface. Used for examples of command-line procedures. Also used to distinguish interface terms, such as names of directories and files, from ordinary text.
<angle brackets>	A term enclosed in angle brackets is a variable placeholder, to be replaced with an appropriate value. Do not enter the angle brackets.
[brackets]	Optional items in command statements. For example, in the following command, [-range <positiveInteger>] means that

Convention	Meaning
	<p>you have the option of entering a range, but it is not required:</p> <p>add lb vserver <name> <serviceType> <IPAddress> <port> [-range <positiveInteger>]</p> <p>Do not type the brackets themselves.</p>
(vertical bar)	<p>A separator between options in braces or brackets in command statements. For example, the following indicates that you choose one of the following load balancing methods:</p> <p><lbMethod> = (ROUNDROBIN LEASTCONNECTION LEASTRESPONSETIME URLHASH DOMAINHASH DESTINATIONIPHASH SOURCEIPHASH SRCIPDESTIPHASH LEASTBANDWIDTH LEASTPACKETS TOKEN SRCIPSRCPORHASH LRTM CALLIDHASH CUSTOMLOAD)</p>
... (ellipsis)	<p>You can repeat the previous item or items in command statements. For example, /route:<DeviceName>[,...] means you can type additional <DeviceNames> separated by commas.</p>

Documentation Available on the NetScaler Appliance

A complete set of Citrix® NetScaler® documentation is available on the **Documentation** tab of your NetScaler appliance and at <http://support.citrix.com/> (PDF version), and at <http://edocs.citrix.com> (HTML version). (The PDF version of the documents require Adobe Reader, available at <http://adobe.com/>.)

To view the documentation

1. From a Web browser, log on to the NetScaler Appliance.
2. Click the **Documentation** tab.
3. To view a short description of each document, hover the mouse pointer over the title. To open a document, click the title.

Getting Service and Support

Citrix® offers a variety of resources for support with your Citrix environment, including the following:

- ♦ The Knowledge Center is a self-service, Web-based technical support database that contains thousands of technical solutions, including access to the latest hotfixes, service packs, and security bulletins.
- ♦ Technical Support Programs for both software support and appliance maintenance are available at a variety of support levels.
- ♦ The Subscription Advantage program is a one-year membership that gives you an easy way to stay current with the latest product version upgrades and enhancements.
- ♦ Citrix Education provides official training and certification programs on virtually all Citrix products and technologies.

For more information about Citrix services and support, see the Citrix Systems Support Web site at <http://www.citrix.com/lang/English/support.asp>.

You can also participate in and follow technical discussions offered by the experts on various Citrix products at the following sites:

- ♦ <http://community.citrix.com>
- ♦ <http://twitter.com/citrixsupport>
- ♦ <http://forums.citrix.com/support>

NetScaler Documentation Feedback

You are encouraged to provide feedback and suggestions so that we can enhance the documentation. You can send an email to nsdocs_feedback@citrix.com. In the subject line, specify "Documentation Feedback." Please include the title of the guide and the page number in the email message.

You can also provide feedback through the Knowledge Center at <http://support.citrix.com/>.

To provide feedback at the Knowledge Center home page

1. Go to the Knowledge Center home page at <http://support.citrix.com/>.
2. On the Knowledge Center home page, under **Products**, expand **NetScaler**, and then click the NetScaler release for which you want to provide feedback.
3. On the **Documentation** tab, click the guide name, and then click **Article Feedback**.
4. On the **Documentation Feedback** page, complete the form, and then click **Submit**.

Chapter 1

Introduction

Topics:

- [Getting Started with the Management Service User Interface](#)
- [Managing the Home Page](#)

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

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

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

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

Getting Started with the Management Service User Interface

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

Logging on to the Management Service User Interface

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

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

To log on to the Management Service user interface

1. In your Web browser address field, type one of the following:
`http://Management Service IP Address`
or
`https://Management Service IP Address`
2. On the **Login** page, in **User Name** and **Password**, type the user name and password of the Management Service. The default user name and password are nsroot and nsroot. However, Citrix recommends that you change the password after initial configuration. For information about changing the nsroot password, see [Changing the Password of the Default User Account](#) on page 20.
3. Click **Show Options**, and then do the following:
 - a. In the **Start in** list, select the page that must be displayed immediately after you log on to the user interface. The available options are Home, Monitoring, Configuration, Documentation, and Downloads. For example, if you want the Management Service to display the Configuration page when you log on, select Configuration in the **Start in** list.
 - b. In **Timeout**, type the length of time (in minutes, hours, or days) after which you want the session to expire. The minimum timeout value is 15 minutes.

The Start in and Timeout settings persist across sessions. Their default values are restored only after you clear the cache.
4. Click **Login** to log on to the Management Service user interface.

Provisioning NetScaler Instances

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

For information about provisioning NetScaler instances, see [Provisioning NetScaler Instances](#) on page 49.

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

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

To log on to a NetScaler instance from the Management Service

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

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

Managing the Home Page

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

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

System Resources

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

System CPU | Memory Usage (%)

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

System WAN/LAN Throughput (Mbps)

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

NetScaler Instances

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

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

Health Monitoring Events

Displays the last 25 events, with their severity, message, source (IP address), and the date and time that the event occurred.

You can do the following on the **Home** page:

View and hide NetScaler instance details

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

Add and remove gadgets

You can also add gadgets to view additional system information.

To add these gadgets, click the arrow (<<) button at the top right corner of the **Home** page, enter keywords in the search box, and then click **Go**. The allowed characters are: a-z, A-Z, 0-9, ^, \$, *, and _. Click **Go** without typing any characters in the search box to display all the gadgets that are available. After the gadget is displayed, click **Add to dashboard**.

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

Hypervisor Details

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

Licenses

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

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

Chapter 2

Managing and Monitoring the NetScaler SDX Appliance

Topics:

- [*Modifying the Network Configuration of the SDX Appliance*](#)
- [*Changing the Password of the Default User Account*](#)
- [*Configuring Clock Synchronization*](#)
- [*SNMP*](#)
- [*Managing Licenses*](#)
- [*Managing Interfaces*](#)
- [*VLAN Filtering*](#)
- [*Viewing the SSL Certificate on the Management Service*](#)
- [*Viewing the Properties of the NetScaler SDX Appliance*](#)
- [*Viewing Real-Time Appliance Throughput*](#)
- [*Viewing Real-Time CPU and Memory Usage*](#)
- [*Viewing CPU Usage for All Cores*](#)
- [*Restarting the Appliance*](#)
- [*Shutting Down the Appliance*](#)
- [*Modifying the Time Zone on the Appliance*](#)
- [*Modifying System Settings*](#)
- [*System Health Monitoring*](#)

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

Modifying the Network Configuration of the SDX Appliance

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

To modify the network configuration of the SDX appliance

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

* A required parameter
4. Click **OK**.

Changing the Password of the Default User Account

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

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

Name

Lists the user accounts configured on the SDX appliance.

Permission

Displays the permission level assigned to the user account.

To change the password of the default user account

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

Configuring Clock Synchronization

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

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

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

To configure an NTP server

1. In the navigation pane, expand **System**, and then click **NTP Servers**.
2. In the details pane, do one of the following:
 - To add a new NTP server, click **Add**.
 - To modify settings for an existing NTP server, select the NTP server, and then click **Open**.
3. In the **Create NTP Server** or **Configure NTP Server** dialog box, set the following parameters:

- **Server Name/IP Address***—The domain name of the NTP server or the IP address of the NTP server. The name or IP address cannot be changed for an existing NTP server.
- **Minimum Poll Interval**— The minimum number of seconds after which the NTP server must poll the NTP messages, expressed as a power of 2. Minimum value: 4 ($2^4=16$ seconds). Maximum value: 6 ($2^6=64$ seconds). Default: 6 ($2^6=64$ seconds).
- **Maximum Poll Interval**— The maximum number of seconds after which the NTP server must poll the NTP messages, expressed as a power of 2. Minimum value: 10 ($2^{10}=1024$ seconds). Maximum value: 17 ($2^{17}=36$ hours). Default : 10 ($2^{10}=1024$ seconds).
- **Key Identifier**—The key to be used for the specified server. This key identifier should be added to the list of Trusted Key IDs in the Authentication Parameters. Minimum value: 1. Maximum value: 65534.

Note: Do not add if Autokey is selected.

- **Autokey**—Use the Autokey protocol for the specified server.
- **Preferred**—Synchronize with this server first. Applicable if more than one server is configured.

*A required parameter

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

To enable NTP synchronization

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

To modify Authentication options

1. In the navigation pane, expand **System**, and then click **NTP Servers**.
2. In the details pane, click **Authentication Parameters**.
3. In the **Modify Authentication Options** dialog box, set the following parameters:
 - **Authentication**—Enable NTP authentication. Possible values: YES, NO. Default: YES.

- **Trusted Key IDs**—The trusted key IDs. While adding an NTP server, you select a key identifier from this list. Minimum value: 1. Maximum value: 65534.
- **Revoke Interval**—The interval between re-randomization of certain cryptographic values used by the Autokey scheme, as a power of 2, in seconds. Default value: 17 ($2^{17}=36$ hours).
- **Automax Interval**—The interval between regeneration of the session key list used with the Autokey protocol, as a power of 2, in seconds. Default value: 12 ($2^{12}=1.1$ hours).

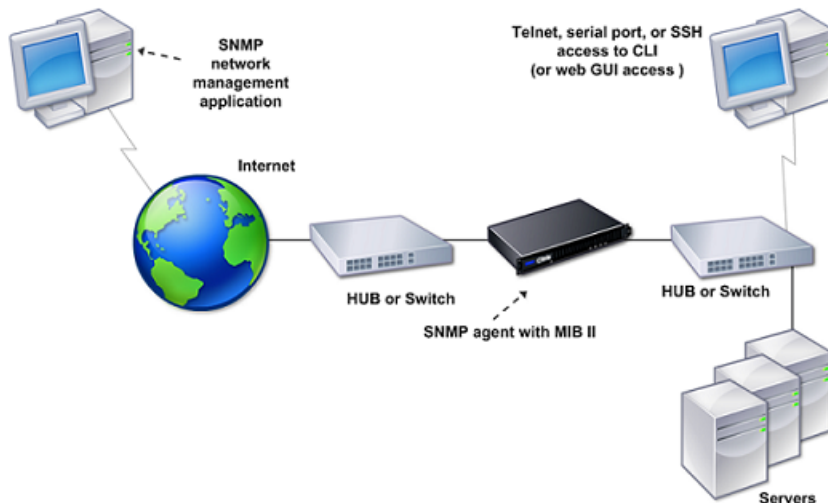
4. Click **OK**, and then click **Close**.

SNMP

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

The following figure illustrates a network with a NetScaler SDX appliance that has SNMP enabled and configured. In the figure, each SNMP network management application uses SNMP to communicate with the SNMP agent on the NetScaler SDX appliance. The SNMP agent searches its management information base (MIB) to collect the data requested by the SNMP Manager and provides the information to the application.

Figure 2-1. NetScaler SDX Appliance Supporting SNMP



SNMP Trap Destinations

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

To add an SNMP trap destination

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

Note: You must specify the same community string on the trap listener device, or the listener drops the messages. Default: public.

4. Click **Add**, and then click **Close**. The SNMP trap destination that you added appears in the **SNMP Traps** pane.

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

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

Downloading MIB Files

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

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

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

To download MIB files

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

Managing Licenses

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

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

Name

The name of the license file.

Last Modified

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

Size

The size of the license file, in bytes.

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

To upload a license file to the SDX appliance

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

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

1. On the **Configuration** tab, in the navigation pane, expand **System**, and then click **Licenses**.
2. In the **License Files** pane, click **Apply Licenses**.

3. In the **Confirm** message box, click **Yes**.

To create a backup by downloading a license file

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

Managing Interfaces

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

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

Port

The interface ID.

State

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

Speed

Specifies the Ethernet speed for the interface, in Mb/s. Possible values: 10, 100, 1000, and 10000.

Duplex

Specifies the duplex setting for the interface. Possible values: Full, Half, NONE. Default: NONE.

To configure an interface

1. On the **Configuration** tab, in the navigation pane, expand **System**, and then click **Interfaces**.
2. In the **Interfaces** pane, click the interface that you want to configure, and then click **Modify**.
3. In the **Modify Interface** dialog box, under **Link Speed** and **Flow Control**, specify values for the following parameters:
 - **Auto Negotiation***—Specifies whether auto-negotiation is enabled on the interface. Possible values: ON, OFF. Default: OFF.
 - **Speed***

- **Duplex***
- **Flow Control Auto Negotiation***—Specifies whether auto-negotiation is performed for flow control parameters.
- **Rx Flow Control***—Specifies whether or not Rx flow control is enabled.
- **Tx Flow Control***—Specifies whether or not Tx flow control is enabled.

* A required parameter

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

To reset the parameters of an interface to their default values

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

VLAN Filtering

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

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

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

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

To enable VLAN filtering on an interface

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

Viewing the SSL Certificate on the Management Service

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

To view the SSL certificate on the Management Service

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

Viewing the Properties of the NetScaler SDX Appliance

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

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

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

Total CPU Cores

The number of CPU cores on the SDX appliance.

Total SSL Cores

The total number of SSL cores on the SDX appliance.

Free SSL Cores

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

Total Memory (GB)

Total appliance memory in gigabytes.

Free Memory (GB)

Free appliance memory in gigabytes.

Hypervisor Uptime

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

Hypervisor Edition

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

Hypervisor Version

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

iSCSI IQN

The iSCSI Qualified Name.

Hypervisor Product Code

The product code of the XenServer.

Hypervisor Serial Number

The serial number of the XenServer.

Hypervisor Build Date

The build date of the XenServer.

Hypervisor Build Number

The build number of the XenServer.

Platform

The hardware platform of the NetScaler SDX appliance, based on the installed license.

Maximum NetScaler Instances

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

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.

Platform

The hardware platform.

Product

The NetScaler product.

Build

The NetScaler build running on the SDX appliance.

IP Address

The IP address of the Management Service.

Host ID

The XenServer host ID.

System ID

The XenServer system ID.

Serial Number

The XenServer serial number.

System Time

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

Uptime

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

BIOS version

BIOS version.

Viewing Real-Time Appliance Throughput

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

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

Viewing Real-Time CPU and Memory Usage

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

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

Viewing CPU Usage for All Cores

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

The **CPU Cores Usage** pane displays the following details:

Core Number

The CPU core number.

CPU Usage

The percent usage of the CPU core.

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

Restarting the Appliance

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

To restart the appliance

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

Shutting Down the Appliance

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

To shut down the appliance

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

Modifying the Time Zone on the Appliance

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

To modify the time zone on the appliance

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

Modifying System Settings

For security reasons, you can specify that the Management Service and a NetScaler VPX instance should communicate with each other only over a secure channel. You can also

restrict access to the Management Service user interface. Clients can log on the Management Service user interface only by using https.

To modify system settings

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

System Health Monitoring

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

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

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

Monitoring the Resources on the SDX Appliance

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

Name

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

Status

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

Current Value

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

Expected Value

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

Monitoring the Storage Resources on the SDX Appliance

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

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

Name

Name of the physical disk.

Size

Size of the disk, in gigabytes (GB).

Utilized

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

Transactions/s

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

Blocks Read/s

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

Blocks Written/s

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

Total Blocks Read

Number of blocks read since the appliance was last started.

Total Blocks Written

Number of blocks written since the appliance was last started.

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

Drive Bay

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

Status

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

- ♦ GOOD: The drive is in a good state and is ready for use.
- ♦ FAIL: The drive has failed and has to be replaced.

- ♦ **MISSING:** A drive is not detected in the drive bay.
- ♦ **UNKNOWN:** A new unformatted drive exists in the drive bay.

Name

System defined name of the storage depository.

Size

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

Utilized

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

Monitoring the Hardware Sensors on the SDX Appliance

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

For fan speed, the following details are displayed:

Name

Name of the fan.

Status

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

Current Value (RPM)

Current rotations per minute.

Temperature information includes the following details:

Name

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

Status

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

Current Value (Degree C)

Current temperature, in degrees, of the component.

Voltage information includes the following details:

Name

Name of the component, such as CPU core.

Status

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

Current Value (Volts)

Current voltage present on the component.

Information about the power supply includes the following details:

Name

Name of the component.

Status

State (condition) of the component. Possible values:

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

Monitoring the Interfaces on the SDX Appliance

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

Interface

Interface number on the SDX appliance.

Status

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

VFs Assigned/Total

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

Tx Packets

Number of packets transmitted since the appliance was last started.

Rx Packets

Number of packets received since the appliance was last started.

Tx Bytes

Number of bytes transmitted since the appliance was last started.

Rx Bytes

Number of bytes received since the appliance was last started.

Tx Errors

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

Rx Errors

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

Chapter 3

Configuring the Management Service

Topics:

- *Managing Client Sessions*
- *Configuring User Accounts*
- *Configuring Policies*
- *SNMP Trap Destinations*
- *Restarting the Management Service*
- *Upgrading the Management Service*
- *Upgrading the XenServer Software*
- *Backing Up and Restoring the Configuration Data of the SDX Appliance*
- *Performing a Factory Reset*
- *Removing Management Service Files*
- *Generating a Tar Archive for Technical Support*

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

Managing Client Sessions

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

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

User Name

The user account that is being used for the session.

IP Address

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

Port

The port being used for the session.

Login Time

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

Last Activity Time

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

Session Expires In

Time left for session expiry.

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

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

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

Configuring User Accounts

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

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

To configure a user account

1. In the navigation pane, expand **System**, and then click **Users**.
The Users pane displays a list of existing user accounts, with their permissions.
2. In the **Users** pane, do one of the following:
 - To create a user account, click **Add**.

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

Default: superuser.

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

To remove a user account

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

Configuring Policies

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

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

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

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

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

To specify the number of backups that the appliance must retain

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

SNMP Trap Destinations

You can use Simple Network Management Protocol (SNMP) to configure the SNMP agent on the Citrix® SDX appliance to generate asynchronous events, which are called *traps*. The traps are generated whenever abnormal conditions occur on the appliance. They are sent to a remote device called a *trap listener*, so that administrators can monitor the appliance and respond promptly to any issues.

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 Management Service user interface.

To add a trap destination

1. In the navigation pane, expand **System**, and then click **SNMP Trap Destinations**.
2. In the **SNMP Trap Destinations** pane, click **Add**.
3. In the **Add SNMP Trap Destination** dialog box, specify values for the following parameters:
 - **Destination Server***—IPv4 address of the trap listener to which to send the SNMP trap messages.

- **Port***—UDP port at which the trap listener listens for trap messages. Must match the setting on the trap listener, or the listener drops the messages. Minimum value: 1. Default: 162.
- **Community***—Password (string) sent with the trap messages, so that the trap listener can authenticate them. Can include letters, numbers, and hyphen (-), period (.) pound (#), 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.

*A required parameter

4. Click **Add**, and then click **Close**. The SNMP trap destination that you added appears in the SNMP Traps pane.

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

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

Restarting the Management Service

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

To restart the Management Service

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

Upgrading the Management Service

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

Uploading the Management Service Build and Documentation Files

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

To upload the Management Service build file

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

To create a backup by downloading a Management Service build file

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

To upload the Management Service documentation file

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

To create a backup by downloading a Management Service documentation file

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

3. In the **Save As** message box, browse to the location where you want to save the file, and then click **Save**.

Upgrading the Management Service to a Later Version

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

To upgrade the Management Service

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

Upgrading the XenServer Software

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

Uploading the XenServer Build Files

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

To upload the XenServer build file

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

To create a backup by downloading a XenServer build file

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

Upgrading the XenServer Software to a Later Version

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

To upgrade the XenServer software

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

Backing Up and Restoring the Configuration Data of the SDX Appliance

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

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

To perform an immediate backup

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

To restore the configuration

1. In the navigation pane, expand **Management Service**, and then click **Backup Files**.
2. In the **Backup Files** pane, click **Restore**.
3. In the **Restore Wizard**, select one of the following:

- **Restore Appliance**—Restores the XenServer, Management Service, and all the NetScaler instances.

Note: Perform a **Factory Reset** before selecting this option.

- All instances—Restores all the NetScaler instances.
 - Specific instances—Restores only the selected NetScaler instances.
4. Click **Next**, and then click **Finish**.
The progress status is displayed.
 5. Click **Close**.

Performing a Factory Reset

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

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

- ♦ Delete NetScaler VPX instances.
- ♦ Delete SSL certificate and key files.
- ♦ Delete license and technical archive files.
- ♦ Delete the NTP configuration on the appliance.
- ♦ Restore the time zone to UTC.
- ♦ Restore prune and backup policies to their default settings.
- ♦ Delete the Management Service image and documentation files.
- ♦ Delete the NetScaler image and documentation files.
- ♦ Delete all XVA images except the last image file that was accessed on the appliance.

- ♦ Restore default interface settings.
- ♦ Restore the default configuration of the appliance, including default profiles, users, and system settings.
- ♦ Restore default IP addresses for XenServer and the Management Service.
- ♦ Restore default passwords for XenServer and the Management Service.
- ♦ Restart the Management Service.

To perform a factory reset

1. In the navigation pane, expand **Management Service**, and then click **Backup Files**.
2. In the **Backup Files** pane, click **Factory Reset**.
3. In the **Factory Reset** dialog box, select the type of reset from the following options:
 - **Reset (Without Network Configuration)**—Retain the IP addresses of the Management Service and XenServer.
 - **Reset (With Network Configuration)**—Management Service and XenServer restart with the default IP addresses.
 - **Appliance Reset**—The appliance settings are restored to the default factory settings, such as default IP addresses for Management Service and XenServer. No instances are installed, and only the default SSL certificate is available on the appliance.
4. Click **OK**, and then click **Close**.

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.

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, in the left pane, expand **Diagnostics**, and then click **Technical Support**.
2. In the **Technical Support** pane, click **Generate Technical Support File**.
3. In the **Generate Technical Support File** dialog box, in **Mode**, specify whether you want to archive data of the XenServer, the Management Service, or both. If you want to archive for both at the same time, select **Appliance**.
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, 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**.

Chapter 4

Provisioning NetScaler Instances

Topics:

- [Creating Admin Profiles](#)
- [Uploading NetScaler .Xva Images](#)
- [Adding a NetScaler Instance](#)

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

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

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

Creating Admin Profiles

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

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

Important:

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

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

To create an admin profile

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

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

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

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

Uploading NetScaler .Xva Images

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

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

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

Name

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

Last Modified

Date when the .xva image file was last modified.

Size

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

To upload a NetScaler .xva file

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

To create a backup by downloading a NetScaler .xva file

1. In the **NetScaler Build Files** pane, select the file that you want to download, and then click **Download**.
2. In the **File Download** message box, click **Save**.

3. In the **Save As** message box, browse to the location where you want to save the file, and then click **Save**.

Adding a NetScaler Instance

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

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

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

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

Name*

The host name assigned to the NetScaler instance.

IP Address*

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

Netmask*

The subnet mask associated with the NSIP address.

Gateway*

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

XVA File*

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

Feature License*

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

Admin Profile*

The profile you want to attach to the NetScaler instance. This profile specifies the administrator (nsroot) user credentials that are used by the Management Service to provision the NetScaler instance and later, to communicate with the instance to retrieve configuration data. The user credentials used in this profile are also used

while logging on to the NetScaler instance by using the GUI or the CLI. It is recommended that you change the default password of the admin profile. This is done by creating a new profile with a user-defined password. For more information, see [Creating Admin Profiles](#) on page 50.

Description

Add a description or comments related to the administrator profile.

Total Memory (MB)*

The total memory allocated to the NetScaler instance.

#SSL Cores*

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

Throughput (Mbps)*

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

Packets per second*

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

CPU

Assign a dedicated core or cores to the instance or the instance shares a core with other instance(s).

Reboot affected Instances if CPU cores are reassigned

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

User Name*

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

Password*

The password for the instance administrator's user name.

Confirm Password*

The password for the instance administrator's user name.

Shell/Sftp/Scp Access*

The access allowed to the NetScaler instance administrator.

Interface Settings

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

Important: The interface IDs of interfaces that you add to an instance do not necessarily correspond to the physical interface numbering on the SDX appliance. For example, if the first interface that you associate with instance 1 is SDX interface

1/4, it appears as interface 1/1 when you log on to the instance and view the interface settings, because it is the first interface that you associated with instance 1.

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

VLAN ID

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

NSVLAN

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

Note:

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

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

Tagged

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

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

Interfaces

Bind the selected interfaces to the VLAN.

To provision a NetScaler instance

1. On the **Configuration** tab, in the navigation pane, expand **NetScaler Configuration**, and then click **Instances**.
2. In the **NetScaler Instances** pane, click **Add**.

3. In the **Provision NetScaler Wizard** follow the instructions on the screen.
4. Click **Create**, and then click **Close**. The NetScaler instance that you provisioned appears in the NetScaler Instances pane.

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 cores, 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.

Chapter 5

Configuring and Managing NetScaler Instances

Topics:

- *Creating a Mapped IP Address or a Subnet IP Address on a NetScaler Instance*
- *Saving the Configuration*
- *Installing SSL Certificates*
- *Upgrading a NetScaler Instance*
- *Managing a NetScaler Instance*
- *Removing NetScaler Instance Files*
- *Applying the Administration Configuration*

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

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

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

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

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

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

To add a MIP or SNIP on a NetScaler instance

1. On the **Configuration** tab, in the navigation pane, click **NetScaler Configuration**.
2. In the **NetScaler Configuration** pane, click **Create IP**.
3. In the **Create NetScaler IP** dialog box, specify values for the following parameters.
 - IP Address***
Specify the IP address assigned as the SNIP or the MIP address.
 - Netmask***
Specify the subnet mask associated with the SNIP or MIP address.
 - Type***
Specify the type of IP address. Possible values: SNIP, MIP. Default value: SNIP.
 - Save Configuration***
Specify whether the configuration should be saved on the NetScaler. Default value is false.
 - Instance IP Address***
Specify the IP address of the NetScaler instance.
4. Click **Create**, and then click **Close**.

Saving the Configuration

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

To save the configuration on a NetScaler instance

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

Installing SSL Certificates

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

Uploading the Certificate File to the SDX Appliance

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

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

Name

The name of the certificate file.

Last Modified

The date when the certificate file was last modified.

Size

The size of the certificate file in bytes.

To upload SSL certificate files to the SDX appliance

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

To create a backup by downloading an SSL certificate file

1. In the **SSL Certificates** pane, select the file that you want to download, and then click **Download**.

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

Uploading SSL Key Files to the SDX Appliance

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

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

Name

The name of the key file.

Last Modified

The date when the key file was last modified.

Size

the size of the key file in bytes.

To upload SSL key files to the SDX appliance

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

To create a backup by downloading an SSL key file

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

Installing an SSL Certificate on a NetScaler Instance

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

To install SSL certificates on a NetScaler instance

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

Certificate File*

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

Key File*

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

Certificate Name*

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

Certificate Format*

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

Password

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

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

Save Configuration*

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

Instance IP Address*

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

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

Upgrading a NetScaler Instance

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

Uploading the NetScaler Software Images, Documentation, and XVA Files and Documentation Files

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

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

Name

Name of the NetScaler instance software image file. The file name contains the release and build number. For example, the file name `build-9.3-53.5_nc.tgz` refers to release 9.3 build 53.5 .

Last Modified

Date when the file was last modified.

Size

Size, in MB, of the file.

To upload a NetScaler software image

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

To create a backup by downloading a NetScaler build file

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

To upload a NetScaler documentation file

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

4. Click **Upload**. The documentation file appears in the **Documentation Files** pane.

To create a backup by downloading a NetScaler documentation file

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

To upload a NetScaler XVA file

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

To create a backup by downloading a NetScaler XVA file

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

Upgrading Multiple NetScaler VPX Instances

You can upgrade the software on the NetScaler VPX instance by using the Management Service. Before you begin upgrading the software, make sure that you have uploaded the correct build and documentation files to the SDX appliance. You can upgrade multiple instances at the same time.

It is important to understand the licensing framework and types of licenses before you upgrade your software. A software edition upgrade may 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.

Note:

- ♦ To prevent any loss of the configuration running on the instance that you want to upgrade, save the configuration on the instance before you upgrade the instance.
- ♦ You can also upgrade an individual instance. To do so, select the instance from the **Instances** node and click **Upgrade**. Click the right arrow at the bottom of the details pane to view the **Upgrade** button.

To upgrade a NetScaler VPX instance image

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

Managing a NetScaler Instance

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

Start a NetScaler Instance

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

Shut down a NetScaler instance

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

Reboot a NetScaler instance

Restart the NetScaler instance.

Delete a NetScaler instance

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

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

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

Removing NetScaler Instance Files

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

To remove NetScaler instance files

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

Applying the Administration Configuration

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

To apply the admin configuration on a NetScaler instance

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

Chapter 6

Monitoring NetScaler Instances

Topics:

- [*Viewing the Properties of the NetScaler Instance*](#)
- [*Viewing the Running and Saved Configuration of a NetScaler Instance*](#)
- [*Pinging a NetScaler Instance*](#)
- [*Tracing the Route of a NetScaler Instance*](#)
- [*Rediscovering a NetScaler Instance*](#)

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

Viewing the Properties of the NetScaler Instance

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

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

To view the properties of NetScaler VPX instances

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

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

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

Name

The host name assigned to the NetScaler instance while provisioning.

VM State

The state of the virtual machine.

NetScaler State

The state of the NetScaler instance.

IP Address

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

Rx (Mbps)

The packets received on the NetScaler instance.

Tx (Mbps)

The packets transmitted by the NetScaler instance.

HTTP Req/s

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

CPU Usage (%)

The percentage of CPU utilization on the NetScaler.

Memory Usage (%)

The percentage of memory utilization on the NetScaler.

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

Netmask

The netmask IP address of the NetScaler instance.

Gateway

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

Packets per second

The total number of packets passing every second.

NICs

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

Version

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

Host Name

The host name of the NetScaler instance.

Total Memory (GB)

The total memory being assigned to the NetScaler instance.

Throughput (Mbps)

The total throughput of the NetScaler instance.

Up Since

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

#SSL Cores

The total number of SSL cores assigned to the instance.

Peer IP address

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

Status

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

HA Master State

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

HA Sync Status

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

Description

The description entered while provisioning the NetScaler instance.

Viewing the Running and Saved Configuration of a NetScaler Instance

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

To view the running and saved configuration of a NetScaler instance

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

Pinging a NetScaler Instance

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

To ping a NetScaler instance

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

Tracing the Route of a NetScaler Instance

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

To trace the route of a NetScaler instance

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

Rediscovering a NetScaler Instance

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

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

To rediscover a NetScaler instance

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

Chapter 7

Using Logs to Monitor Operations and Events

Topics:

- [Viewing Audit Logs](#)
- [Viewing Task Logs](#)
- [Viewing Events](#)

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

Viewing Audit Logs

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

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

To view audit logs

1. In the navigation pane, expand **System**, and then click **Audit**.

2. In the **Audit Log** pane, you can view the following details.

User Name

The Management Service user who has performed the operation.

IP Address

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

Port

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

Resource Type

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

Resource Name

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

Audit Time

The time when the audit log was generated.

Operation

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

Status

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

Message

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

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

Viewing Task Logs

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

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

To view the task log

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

ID

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

Name

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

Status

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

Executed By

The Management Service user who has performed the operation.

Start Time

The time at which the task started.

End Time

The time at which the task ended.

- 3.

Viewing Task Device Logs

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

To view the task device log

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

Viewing Task Command Logs

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

To view the task command log

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

Viewing Events

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

To view the events

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

Severity

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

Source

The IP address on which the event is generated.

Date

The date when the event is generated.

Category

The category of event, such as PolicyFailed and DeviceConfigChange.

Message

The message describing the event.

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

Chapter 8

Use Cases for NetScaler SDX Appliance

Topics:

- *Consolidation When the Management Service and the NetScaler Instances are in the Same Network*
- *Consolidation When the Management Service and the NetScaler Instances are in Different Networks*
- *Consolidation Across Security Zones*

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

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

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

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

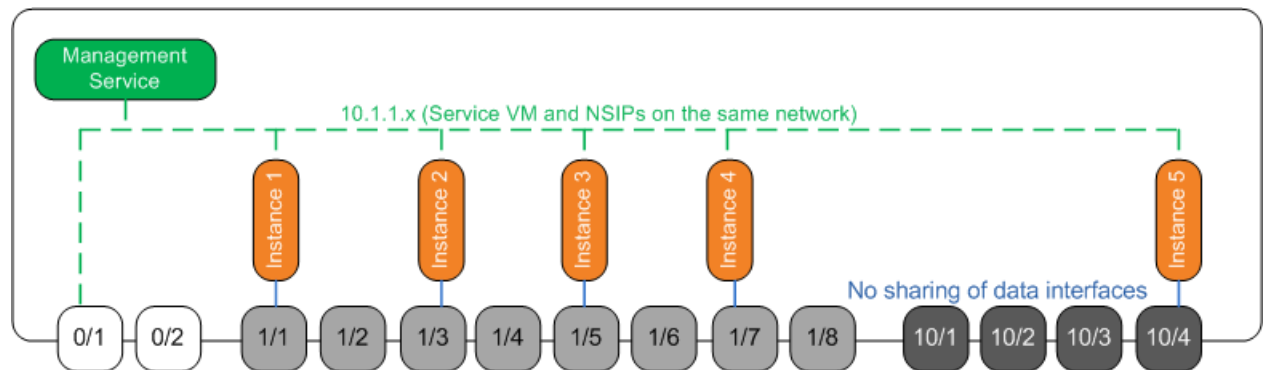
Consolidation When the Management Service and the NetScaler Instances are in the Same Network

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

In the following example, the Management Service and the NetScaler instances are part of the 10.1.1.x. network. Interfaces 0/1 and 0/2 are the management interfaces, 1/1 to 1/8 are 1G data interfaces, and 10/1 to 10/4 are 10G data interfaces. Each instance has its own dedicated physical interface. Therefore, the number of instances is limited to the number of physical interfaces available on the appliance. By default, VLAN filtering is enabled on each interface of the NetScaler SDX appliance, and that restricts the number of VLANs to 32 on a 1G interface and 63 on a 10G interface. VLAN filtering can be enabled and disabled for each interface. Disable VLAN filtering to configure up to 4096 VLANs per interface on each instance. In this example, VLAN filtering is not required because each instance has its own dedicated interface. For more information about VLAN filtering, see [VLAN Filtering](#) on page 27.

The following figure illustrates the above use case.

Figure 8-1. Network topology of an SDX appliance with Management Service and NetScaler NSIPs for instances in the same network



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

Parameter Name	Values for Instance 1
Name	vpx8
IP Address	10.1.1.2
Netmask	255.255.255.0
Gateway	10.1.1.1
XVA File	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature License	Platinum
Admin Profile	ns_nsroot_profile
User Name	vpx8
Password	Sdx
Confirm Password	Sdx
Shell/Sftp/Scp Access	True
Total Memory (MB)	2048
#SSL Cores	1
Throughput (Mbps)	1000
Packets per second	1000000
CPU	Shared
Interface	0/1 and 1/1

To provision NetScaler Instance 1 as shown in this example

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

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

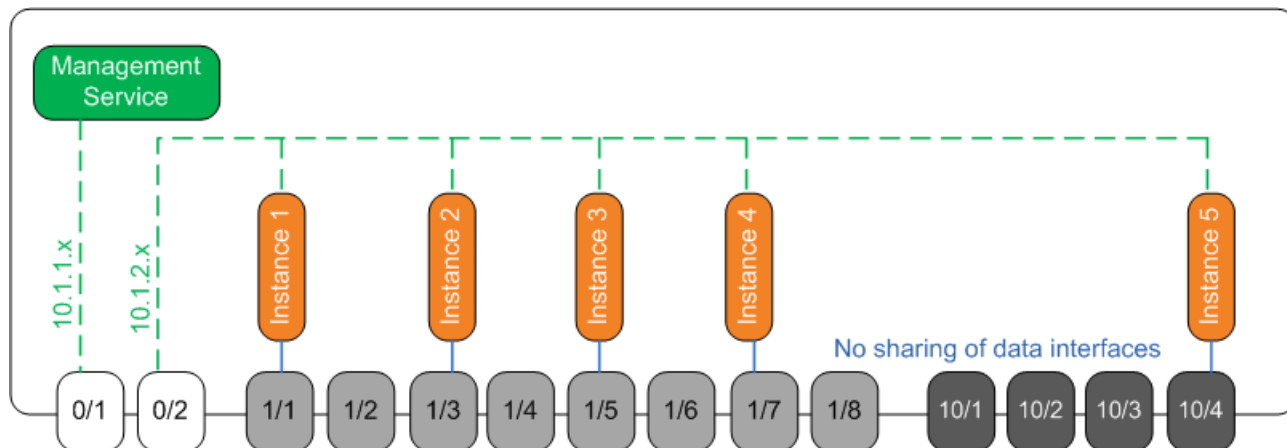
Consolidation When the Management Service and the NetScaler Instances are in Different Networks

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

In the following example, the Management Service is in the 10.1.1.x network and the NetScaler instances are in the 10.1.2.x network. Interfaces 0/1 and 0/2 are the management interfaces, 1/1 to 1/8 are 1G data interfaces, and 10/1 to 10/4 are 10G data interfaces. Each instance has its own dedicated administrator and its own dedicated physical interface. Therefore, the number of instances is limited to the number of physical interfaces available on the appliance. VLAN filtering is not required, because each instance has its own dedicated interface. Optionally, disable VLAN filtering to configure up to 4096 VLANs per instance per interface. In this example, you do not need to configure an NSVLAN, because instances are not sharing a physical interface and there are no tagged VLANs. For more information about NSVLANs, see [Adding a NetScaler Instance](#) on page 52.

The following figure illustrates the above use case.

Figure 8-2. Network topology of an SDX appliance with Management Service and NetScaler NSIPs for Instances in different networks



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

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

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

To provision NetScaler Instance 1 as shown in this example

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

Consolidation Across Security Zones

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

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

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

Note: Tagging is supported in XenServer version 6.0.

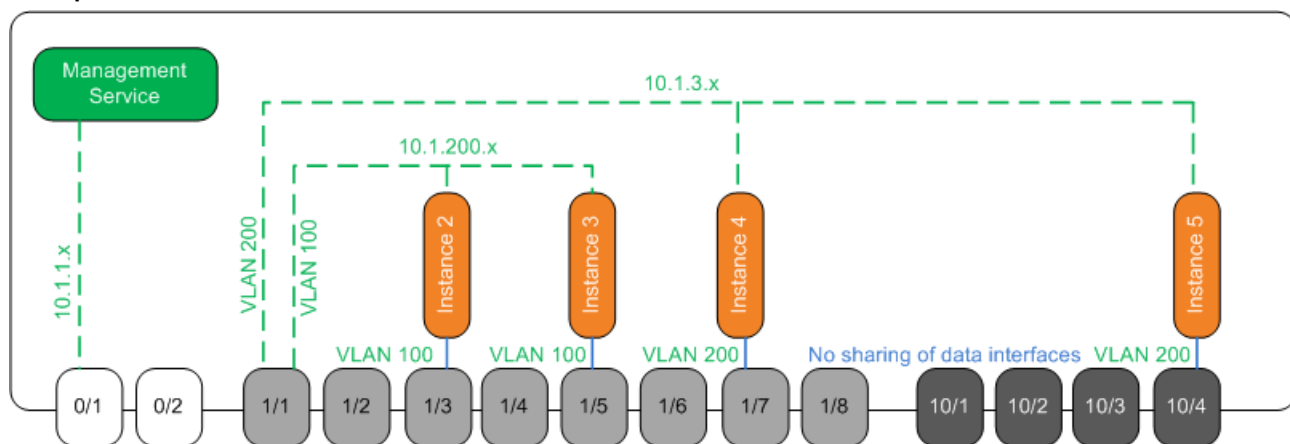
Consolidation with Dedicated Interfaces for Each Instance

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

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

The following figure illustrates the above use case.

Figure 8-3. Network topology of an SDX appliance with NetScaler instances in multiple networks



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

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

Parameter Name	Values for Instance 5	Values for Instance 3
Name	vpx5	vpx3
IP Address	10.1.3.2	10.1.200.2
Netmask	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.200.1

Parameter Name	Values for Instance 5	Values for Instance 3
XVA File	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature License	Platinum	Platinum
Admin Profile	ns_nsroot_profile	ns_nsroot_profile
User Name	vp5	vp3
Password	Sdx	root
Confirm Password	Sdx	root
Shell/Sftp/Scp Access	True	True
Total Memory (MB)	2048	2048
#SSL Cores	1	1
Throughput (Mbps)	1000	1000
Packets per second	1000000	1000000
CPU	Shared	Shared
Interface	1/1 and 10/4	1/1 and 1/5
NSVLAN	200	100
Add (interface)	1/1	1/1
Tagged Interface	Select Tagged	Select Tagged

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

1. On the **Configuration** tab, in the navigation pane, expand **NetScaler Configuration**, and then click **Instances**.
2. In the **NetScaler Instances** pane, click **Add**.

3. In the **Provision NetScaler Wizard** follow the instructions in the wizard to set the parameters to the values shown in the above table.
4. Click **Create**, and then click **Close**. The NetScaler instance you provisioned appears in the NetScaler Instances pane.

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

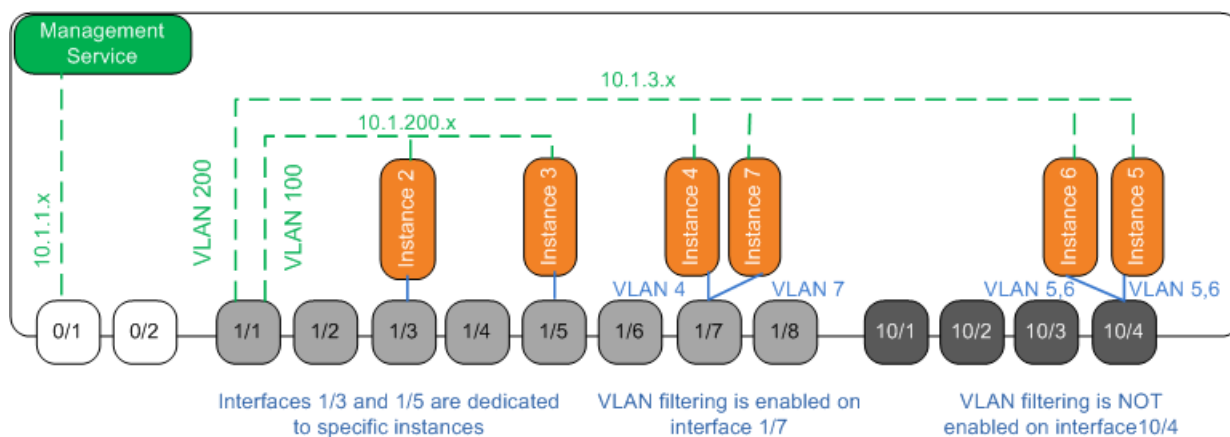
You can enable and disable VLAN filtering on an interface as required. For example, if you need to configure more than 100 VLANs on an instance, assign a dedicated physical interface to that instance and disable VLAN filtering on that interface. Enable VLAN filtering on instances that share a physical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

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

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

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

The following figure illustrates the above use case.

Figure 8-4. Network topology of an SDX appliance with Management Service and NetScaler instances distributed across networks

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

Parameter Name	Values for Instance 7	Values for Instance 4
Name	vp7	vp4
IP Address	10.1.3.7	10.1.3.4
Netmask	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.3.1
XVA File	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature License	Platinum	Platinum
Admin Profile	ns_nsroot_profile	ns_nsroot_profile
User Name	vp4	vp4
Password	Sdx	Sdx
Confirm Password	Sdx	Sdx
Shell/Sftp/Scp Access	True	True

Parameter Name	Values for Instance 7	Values for Instance 4
Total Memory (MB)	2048	2048
#SSL Cores	1	1
Throughput (Mbps)	1000	1000
Packets per second	1000000	1000000
CPU	Shared	Shared
Interface	1/1 and 1/7	1/1 and 1/7
NSVLAN	200	200

To provision NetScaler Instances 7 and 4 in this example

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