



Juniper Networks Network and Security Manager

Installation Guide

Release

2012.1



Modified: 2019-05-30

Revision 4

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Network and Security Manager Installation Guide
Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Revision History
May 2019—Revision 4

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About This Guide	xv
	Objectives	xv
	Audience	xv
	Conventions	xv
	Documentation	xvii
	Requesting Technical Support	xix
	Self-Help Online Tools and Resources	xix
	Creating a Service Request with JTAC	xx
Part 1	Network and Security Manager Installation Procedures	
Chapter 1	Introduction	3
	Installation Process Overview	3
	Management System Installation Process	3
	User Interface Installation Process	4
	Installation Package	4
	Minimum System Requirements	5
	System Requirements—Management System	5
	System Requirements—User Interface	7
	Choosing Standalone, Distributed, or High Availability Configurations	8
	Standalone Configuration	9
	Distributed Configuration	9
	Simple High Availability Configuration	9
	Extended High Availability Configuration	10
	Other Configuration Options	10
	Local/Remote Database Backup	10
	NetScreen-Statistical Report Server Interoperability	11
	Device Server Database	11
	Next Steps	12
Chapter 2	Installing NSM in a Standalone Configuration	15
	Suggested Standalone Configuration Installation Order	15
	Defining System Parameters	16
	Prerequisite Steps	19
	Running the System Update Utility	20
	Configuring Shared Memory Size	20
	Establishing a Trust Relationship	21
	Establishing a Trust Relationship on a High Availability Cluster	22
	Preparing a Solaris Server for NSM	23

	Installing NSM 2012.2	24
	Typical Output for a Standalone Installation	31
	Installing NSM with an IPv6 Management Address	35
	Starting Server Processes Manually	39
	Validating Management System Status	39
	Installing the User Interface	39
	Running the User Interface	45
	Validating the NSM Installation	46
	Running the User Interface in Demo Mode	47
	Next Steps	47
Chapter 3	Installing NSM in a Distributed Configuration	49
	Suggested Distributed Configuration Installation Order	49
	Defining System Parameters	50
	Prerequisites	53
	Installing the GUI Server	53
	Typical Output for Installing a GUI Server in a Distributed Configuration	59
	Installing the User Interface	62
	Adding the Device Server in the User Interface	63
	Installing the Device Server	63
	Typical Output for Installing a Device Server in a Distributed Configuration	66
	Installing NSM with an IPv6 Management Address	69
	Primary GUI Server Output	70
	Primary Dev Server Output	74
	Starting Server Processes Manually	78
	Validating Management System Status	78
	Next Steps	78
Chapter 4	Installing NSM with High Availability	79
	High Availability Overview	79
	HA Configuration Options	80
	HA Requirements	80
	Communication Between Physical Servers	81
	Inter-server Communications	81
	HA Server	81
	Database Synchronization and Remote Replication	82
	HA Failover	82
	Restoring Connections	84
	Using a Shared Disk	84
	Creating a Trust Relationship Between Servers	85
	Server Authentication	85
	Checking HA Status	85
	Viewing HA Error Logs	85
	HA Utilities	86
	Suggested Simple HA Installation Order	86
	Suggested Extended HA Installation Order	87
	Defining System Parameters	88
	Simple HA Configuration Parameters	88
	Extended HA Configuration Parameters	91

Shared Disk Parameters	92
Prerequisites	92
Verifying That Shared Partitions Are Mounted Properly	93
Verifying That All Required System Binaries Are Available	93
Verifying That Clocks Are Synchronized	93
Establishing an SSH Trust Relationship	93
Installing NSM 2012.2 on the Primary Server	95
Viewing the Management System Installation Log	102
Installing NSM with an IPv6 Management Address	102
Starting Server Processes Manually	107
Validating Management System Status	108
Other Useful Commands	108
Installing NSM 2012.2 on the Secondary Server	109
Example: Installing NSM in a Simple HA Configuration	109
Primary GUI Server and Device Server Installation	110
Secondary GUI Server and Device Server Installation Script	115
Installing the User Interface	121
Configuring the HA Cluster in the UI	121
Installing NSM In an Extended HA Configuration	124
Example: Installing NSM in an Extended HA Configuration	125
Primary GUI Server Installation Script	126
Secondary GUI Server Installation	131
Primary Device Server Installation	135
Secondary Device Server Installation	140
Next Steps	144
Chapter 5	
Upgrading to NSM 2012.2 from an Earlier Version	145
Upgrade Overview	145
PostgreSQL Database Upgrade from 8.1.7 to 8.4.10	146
Upgrading PostgreSQL and Migrating to NSM 2012.2	146
System Update	146
Migrate NSM to 2012.2 NSM Release	147
Using SQL Tools	148
Defining System Parameters	149
Standalone Configuration Parameters	149
Distributed Configuration Parameters	151
HA Configuration Parameters	151
Shared Disk Parameters	153
Prerequisite Steps	154
Running the System Update Utility	155
Configuring Shared Memory Size	155
Setting the rsync Timeout Values	156
Increasing Shared Memory Segment Maximum Size	156
Preparing a Solaris Server for NSM	157
Upgrading NSM in a Standalone Configuration	158
Typical Output for a Standalone Upgrade	163
Installing NSM with an IPv6 Management Address	166
Starting Server Processes Manually	169
Validating Management System Status	169

	Upgrading the User Interface	170
	Downloading and Installing the UI Client Automatically	170
	Downloading and Installing the UI Client Manually	170
	Validating the Upgrade	171
	Upgrading NSM in a Distributed Configuration	171
	Installing NSM with IPv6 Management addresses	172
	Primary GUI Server Output	172
	Primary Dev Server Output	176
	Upgrading NSM with HA Enabled	180
	Typical Output with HA Enabled for IPv6 Management address	182
	Upgrading the Database Backup Files	187
	Restoring Data if the Upgrade Fails	188
	Next Steps	188
Chapter 6	Upgrading NSM Appliances to NSM 2012.2	189
	Prerequisite Steps	189
	Upgrading an NSM Appliance in a Standalone Setup	190
	Upgrading NSM Regional Server and NSM CM Appliances Using Specific Files	196
	Upgrading to NSM Release 2012.2 on an NSM Regional Server Appliance (Online mode)	196
	Upgrading to NSM 2012.2 Release on an NSM Central Manager Appliance (Online mode)	199
	Upgrading to NSM 2012.2 Release on an NSM Regional Server Appliance (Offline Mode)	202
	Upgrading to NSM Release 2012.2 on an NSM Central Manager Appliance (Offline Mode)	206
	Upgrading an NSM Appliance in an HA Setup	208
	Upgrading an NSM Appliance in an Extended HA Setup	218
	Migrating Data to an NSM Regional Server Appliance	225
	Data Migration from a Solaris Server to an NSM Regional Server Appliance	225
	On the Solaris server:	226
	On the NSM appliance:	226
	Data Migration from a Linux Server to an NSM Regional Server Appliance	228
	On the Linux Server	228
	On the NSMAppliance	229
	User Privileges on an NSM Appliance	230
Chapter 7	Upgrading CentOS 4.x to CentOS 5.7 on NSM Appliances	233
	Upgrading an NSM Appliance OS	233
	Upgrade Using Local Hard disk	233
	Upgrading Using CDROM	235
	Setting Up Administrative Accounts and Networking	236
	Logging In to the System	236
	Connecting an Appliance to the Network	236
	Configuring and Installing NSM	236

	Running NSM Setup	237
	Sub Option Choice [1-10,Q,R]: 5	237
	Sub Option Choice [1-9,Q,R]: 9	237
	Sub Option Choice 1 - Typical Setting	238
	Choice [1-6,A,C,R]: 2	238
	Choice [1-6,A,C,R]: 3	239
	Choice [1-6,A,C,R]: 4	240
	Choice [1-6,A,C,R]: 5	240
	Choice [1-2,M,R]: 1	241
	Choice [1-6,A,C,R]: A	241
	Checking the Installation	244
	Tested CentOS Upgrade Paths	245
	Scenario 1	246
	Scenario 2	246
	Scenario 3	246
	Scenario 4	247
	Scenario 5	247
	Scenario 6	247
	Scenario 7	247
	Scenario 8	248
	Scenario 9	248
	Scenario 10	249
Chapter 8	Maintaining NSM	251
	Controlling the Management System	251
	Viewing Management System Commands	251
	Common Management System Commands	252
	Starting All Server Processes Using the HA Server	252
	Starting GUI Server and Device Server Processes Manually	253
	Stopping Server Processes	253
	Configuring Server Options	254
	Changing the Management System IP Address	254
	Changing the Device Server IP Address	255
	Changing the GUI Server IP Address	255
	Configuring Disk Space Management on the Device Server	255
	Configuring Disk Space Management on the GUI Server	256
	Configuring Connection Timing	257
	Setting Core File Naming on Solaris	258
	Archiving and Restoring Logs and Configuration Data	258
	Archiving Logs and Configuration data	258
	Restoring Logs and Configuration Data	260
	Configuring High Availability Options	260
	Enabling and Disabling High Availability Processes	261
	Configuring Other High Availability Options	261
	Backing Up the Database Locally	262
	Restoring the Database	262
	Validating the Database Recovery Process	263
	Changing the HA Server IP Address	263

	Relocating the Database	263
	Archiving the GUI Server Database and Device Server Log Database	264
	Installing NSM On a New System	264
	Moving the Databases to the New System	264
	Installing a Trivial File Transfer Protocol Server	267
	Installing a TFTP Server on Linux	267
	Installing a TFTP Server on Solaris	268
	Modifying Timeout Values on the Device Server	268
	Downgrade Procedures	269
	Removing the Management System	270
	Uninstalling the User Interface	271
Part 2	Appendixes	
Appendix A	Technical Overview of the NSM Architecture	275
	About the Management System	276
	GUI Server	276
	Device Server	277
	HA Server	277
	About the NSM User Interface	277
	About Managed Devices	277
	Server Communications	277
	Communication Ports and Protocols	278
	Using the Secure Server Protocol	279
	Communications with Devices Running ScreenOS 5.X and Later	280
	Communications with Device Management Interface-Compatible Devices	281
	Creating a Separate Management Network	281
Appendix B	Hardware Recommendations	283
	Standalone or Distributed System for GUI Server and Device Server	283
	Network Card Requirements	284
	Configuring Multiple Network Interface Cards	284
	Memory Requirements	284
	GUI Server	284
	Device Server	285
	UI Client	286
	Storage Space Requirements	286
	GUI Server	286
	Audit Log	286
	Error Log	288
	Device Configuration Database	288
	Nightly Backup	288
	Device Server Requirements	288
	Processor Speed Requirements	289
	GUI Server	289
	Device Server Managing IDP Standalone Devices Running Profiler	289
	Recommendations for Large-Scale Installations	290

Appendix C	Profiler Performance Tuning Recommendations	291
	Performance Tuning Recommendations	291
	Recommendations for Low-End Configurations:	291
	Medium-Size Configuration (3 to 8 IDP Profiling Devices)	292
	High-End Configuration (9 to 20 IDP Profiling Devices)	293
	Setting Preferences to Improve Profiler Performance	294
	UI System Preferences	294
	PostgreSQL Server	295
	Shared Memory	295
	Device Server	296
	NSM Generated Logs' Impact on Performance	297
	GUI Server	298

List of Figures

Part 1	Network and Security Manager Installation Procedures	
Chapter 2	Installing NSM in a Standalone Configuration	15
	Figure 1: UI Installer Introduction Screen	41
	Figure 2: UI Installation—Choose Install Folder	42
	Figure 3: UI Installation—Choose Shortcut Folder	43
	Figure 4: UI Installation—Preinstallation Summary	44
	Figure 5: Validating the NSM Installation	46
Chapter 4	Installing NSM with High Availability	79
	Figure 6: Simple HA Management System Configuration	80
	Figure 7: HA Configuration Example	110
	Figure 8: Configuring the HA GUI Server Cluster	122
	Figure 9: Configuring the HA Device Server Cluster	123
	Figure 10: Configuring e-mail Notification	124
	Figure 11: Extended HA Configuration Example	126
Chapter 5	Upgrading to NSM 2012.2 from an Earlier Version	145
	Figure 12: Update Script	147
	Figure 13: Installer Script	148
	Figure 14: Upgrade Confirmation Message	148
Part 2	Appendixes	
Appendix A	Technical Overview of the NSM Architecture	275
	Figure 15: NSM Architecture	275
	Figure 16: NSM Management System	276

List of Tables

	About This Guide	xv
	Table 1: Notice Icons	xvi
	Table 2: Text Conventions	xvi
	Table 3: Syntax Conventions	xvii
	Table 4: Network and Security Manager Publications	xvii
Part 1	Network and Security Manager Installation Procedures	
Chapter 1	Introduction	3
	Table 5: NSM Installation Files	4
	Table 6: Minimum System Requirements—Management System on Same Server	5
	Table 7: Minimum System Requirements—Management System on Separate Servers	6
	Table 8: Minimum System Requirements—User Interface	7
Chapter 2	Installing NSM in a Standalone Configuration	15
	Table 9: Common System Parameters	17
Chapter 3	Installing NSM in a Distributed Configuration	49
	Table 10: Distributed Configuration—System Parameters	51
Chapter 4	Installing NSM with High Availability	79
	Table 11: HA Utilities	86
	Table 12: Simple HA Configuration—System Parameters	88
	Table 13: Extended HA Configuration—System Parameters	91
	Table 14: Shared Disk System Parameters	92
	Table 15: Useful Installation and Troubleshooting Commands	108
Chapter 5	Upgrading to NSM 2012.2 from an Earlier Version	145
	Table 16: Standalone Configuration—System Parameters	149
	Table 17: Distributed Configuration — System Parameters	151
	Table 18: HA Configuration — System Parameters	151
	Table 19: Shared Disk Parameters	153
Chapter 6	Upgrading NSM Appliances to NSM 2012.2	189
	Table 20: Files for Offline Upgrade	191
	Table 21: Files for Offline Upgrade	210
	Table 22: Files for Offline Upgrade	219
Chapter 8	Maintaining NSM	251
	Table 23: Management System Commands	252

Part 2	Appendixes
Appendix A	Technical Overview of the NSM Architecture 275
	Table 24: Inbound ports on the NSM Management System 278
	Table 25: Outbound ports on the NSM Management System 279
	Table 26: Management System Communications With Devices Running ScreenOS 280
	Table 27: Management System Communications With DMI-Compatible Devices 281
Appendix B	Hardware Recommendations 283
	Table 28: GUI Server RAM Requirements 284
	Table 29: Device Server RAM Requirements for Firewall/VPN or Junos Devices 285
	Table 30: Device Server RAM Requirements for IDP, Secure Access, or Infranet Controller Devices 285
	Table 31: Audit Log Details 287
	Table 32: Storage Requirements for Device Server Managing Firewall/VPN Devices 288
	Table 33: Storage Requirements for Device Server Managing IDP (w/Profiler) Devices 289
	Table 34: CPU Requirements for Device Server Managing IDP (w/Profiler) Devices 289
Appendix C	Profiler Performance Tuning Recommendations 291
	Table 35: Performance Turning Recommendations for Low-End Configurations 291
	Table 36: Performance Turning Recommendations for Medium-Sized Configurations 292
	Table 37: Performance Turning Recommendations for High-End Configurations 293
	Table 38: Profiler Settings in UI System Preferences 294
	Table 39: PostgreSQL Server Settings 295
	Table 40: Device Server Settings 296

About This Guide

- [Objectives on page xv](#)
- [Audience on page xv](#)
- [Conventions on page xv](#)
- [Documentation on page xvii](#)
- [Requesting Technical Support on page xix](#)

Objectives

This *Network and Security Manager Installation Guide* describes how you can install an initial working Network and Security Manager (NSM) system.

Audience

This guide is intended primarily for IT administrators who are responsible for installing, upgrading, and maintaining NSM.

Conventions

The sample screens used throughout this guide are representations of the screens that appear when you install and configure the NSM software. The actual screens may differ.

All examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

[Table 1 on page xvi](#) defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xvi defines text conventions used in this guide.

Table 2: Text Conventions

Convention	Description	Examples
Bold typeface like this	<ul style="list-style-type: none"> Represents commands and keywords in text. Represents keywords Represents UI elements 	<ul style="list-style-type: none"> Issue the clock source command. Specify the keyword exp-msg. Click User Objects
Bold typeface like this	Represents text that the user must type.	user input
<code>fixed-width font</code>	Represents information as displayed on the terminal screen.	<pre>host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</pre>
Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d
<i>Italics</i>	<ul style="list-style-type: none"> Emphasizes words Identifies variables 	<ul style="list-style-type: none"> The product supports two levels of access, <i>user</i> and <i>privileged</i>. <i>clusterID</i>, <i>ipAddress</i>.

Table 2: Text Conventions (continued)

Convention	Description	Examples
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	Object Manager > User Objects > Local Objects

Table 3 on page xvii defines syntax conventions used in this guide.

Table 3: Syntax Conventions

Convention	Description	Examples
Words in plain text	Represent keywords	terminal length
Words in italics	Represent variables	<i>mask, accessListName</i>
Words separated by the pipe () symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.	diagnostic line
Words enclosed in brackets ([])	Represent optional keywords or variables.	[internal external]
Words enclosed in brackets followed by an asterisk ([]*)	Represent optional keywords or variables that can be entered more than once.	[level1 level2 11]*
Words enclosed in braces ({ })	Represent required keywords or variables.	{ permit deny } { in out } { clusterId ipAddress }

Documentation

Table 4 on page xvii describes documentation for NSM.

Table 4: Network and Security Manager Publications

Book	Description
<i>Network and Security Manager Installation Guide</i>	Describes the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation or upgrade of NSM.

Table 4: Network and Security Manager Publications (continued)

Book	Description
<i>Network and Security Manager Administration Guide</i>	<p>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI.</p> <p>This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</p>
<i>Network and Security Manager Configuring ScreenOS Devices Guide</i>	Provides details about configuring device features for all supported ScreenOS platforms.
<i>Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide</i>	Provides details about configuring device features for all supported Intrusion Detection and Prevention (IDP) platforms.
<i>Network and Security Manager Online Help</i>	Provides procedures for basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.
<i>Network and Security Manager API Guide</i>	Provides complete syntax and description of the SOAP messaging interface to NSM.
<i>Network and Security Manager Release Notes</i>	<p>Provides the latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the Release Notes differs from the information found in the documentation set, follow the Release Notes.</p> <p>Release notes are included on the corresponding software CD and are available on the Juniper Networks website.</p>
<i>Network and Security Manager Configuring Infranet Controllers Guide</i>	Provides details about configuring the device features for all supported Infranet Controllers.
<i>Network and Security Manager Configuring Secure Access Devices Guide</i>	Provides details about configuring the device features for all supported Secure Access Devices.
<i>Network and Security Manager Configuring EX Series Switches Guide</i>	Provides details about configuring the device features for all supported EX Series platforms.

Table 4: Network and Security Manager Publications (continued)

Book	Description
<i>Network and Security Manager Configuring J Series Services Routers and SRX Series Services Gateways Guide</i>	Provides details about configuring the device features for all supported J Series Services Routers and SRX Series Services Gateways.
<i>Network and Security Manager M Series and MX Series Devices Guide</i>	Provides details about configuring the device features for M Series and MX Series platforms.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

PART 1

Network and Security Manager Installation Procedures

- [Introduction on page 3](#)
- [Installing NSM in a Standalone Configuration on page 15](#)
- [Installing NSM in a Distributed Configuration on page 49](#)
- [Installing NSM with High Availability on page 79](#)
- [Upgrading to NSM 2012.2 from an Earlier Version on page 145](#)
- [Upgrading NSM Appliances to NSM 2012.2 on page 189](#)
- [Upgrading CentOS 4.x to CentOS 5.7 on NSM Appliances on page 233](#)
- [Maintaining NSM on page 251](#)

CHAPTER 1

Introduction

This chapter provides you with the information you need to install Network and Security Manager (NSM) and integrate it into your network. It provides an overview of the NSM installation process. It also reviews minimum hardware and software requirements and options for configuring the management system to provide enhanced functionality, performance, and scalability.

This chapter contains the following sections:

- [Installation Process Overview on page 3](#)
- [Installation Package on page 4](#)
- [Minimum System Requirements on page 5](#)
- [Choosing Standalone, Distributed, or High Availability Configurations on page 8](#)
- [Other Configuration Options on page 10](#)
- [Next Steps on page 12](#)

Installation Process Overview

NSM is software that enables you to integrate and centralize management of your Juniper Networks environment.

You need to install two main software components that you need to install to run NSM: the NSM management system and the NSM user interface (UI).

The overall process for installing NSM is as follows:

- [Management System Installation Process on page 3](#)
- [User Interface Installation Process on page 4](#)

Management System Installation Process

The management system installer enables you to install all the software required to run each component of the NSM management system.

The management system installer is a shell archive script that you can run on any of the following dedicated platforms that meets minimum requirements:

- Solaris 10 (for SPARC)

- Red Hat Enterprise Linux (RHEL) ES/AS 4.0 or ES/AS 5.0 (Minimal and Full Install)

See [“Minimum System Requirements” on page 5](#) for more information on the minimum required hardware and software that you need to install the NSM management system. To plan for larger deployments, refer to [“Hardware Recommendations” on page 283](#).



NOTE: NSM 2008.1 and later no longer support installations on servers running Solaris 8 or 9. If you plan to install the management system on a server running Solaris 8 or 9, you must upgrade the system to Solaris 10. Similarly, NSM 2008.1 and later no longer support installations on RHEL ES/AS 3.0. If you plan to install the management system on a server running RHEL ES/AS 3.0, you must upgrade the system to either RHEL ES/AS 4.0 or RHEL ES/AS 5.0.

RHEL and Solaris installations use different installer scripts. When you launch the management system installer, the NSM installer guides you through all the steps required to install and configure each management system component.

User Interface Installation Process

The NSM user interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based that meets minimum system requirements. See [Table 8 on page 7](#) for more information on the minimum required hardware and software that you need to install the NSM UI.

The InstallAnywhere wizard guides you through all the steps required to configure and install the UI. After you install the UI, you can connect it to the management system.

Installation Package

All the software files required to install NSM are available on the Internet at the [Juniper Networks web site](#). We recommend you download these files to the computers on which you plan to install NSM before you begin the installation process.

[Table 5 on page 4](#) describes the contents of the NSM installation package.

Table 5: NSM Installation Files

Filename	Description
nsm2012.2_ui_win_x86.exe	Installer for the NSM UI (for Windows-based computers).
nsm2012.2_ui_linux_x86.bin	Installer for the NSM UI (for Linux-based computers).
nsm2012.2_servers_linux_x86.sh	Installer for the NSM management system for Linux.
nsm2012.2_servers_sol_sparc.sh	Installer for the NSM management system for Solaris.

Table 5: NSM Installation Files (continued)

Filename	Description
<code>nsm2012.2-systemupdate-linuxES_4.tar</code>	System update utility for RHEL ES 4.0. Use this file to update files on your system required for the NSM installer to run properly.
<code>nsm2012.2-systemupdate-linuxES_5.tar</code>	System update utility for RHEL ES 5.0. Use this file to update files on your system required for the NSM installer to run properly.
<code>nsm2012.2-systemupdate-solaris10.tar</code>	System update utility for Solaris 10. Use this file to update files on your system required for the NSM installer to run properly.

Minimum System Requirements

The following minimum hardware and software requirements must be met to properly install and run NSM.

System Requirements—Management System

[Table 6 on page 5](#) describes the minimum requirements that must be met for the GUI server and Device server on the same server.

Table 6: Minimum System Requirements—Management System on Same Server

Component	Requirements
Operating System	Solaris 10 operating system with End User Solaris Software Group package, or RHEL 32-bit ES/AS 4.0-Update 8 or 32-bit ES/AS 5.0-Update 4 (Minimal and Full Install) RHEL 32-bit ES 6.5
CPU	Only Sun Microsystems UltraSPARC III (Cu) 1.2 GHz or UltraSPARC T2, or Linux 2 GHz (x86) processor (or higher)
RAM	4 GB
Swap Space	4 GB for both GUI server and Device server
Storage	Hard disk drive with 7200 RPM (minimum); 15,000 RPM (recommended); 40 GB disk space (minimum); 80 GB disk space (recommended) By directory: <ul style="list-style-type: none"> • <code>/usr</code>—7 GB minimum • <code>/var</code>—10 GB min • <code>/tmp</code>—2 GB minimum

Table 6: Minimum System Requirements—Management System on Same Server (continued)

Component	Requirements
Network Connection	100 Mbps (minimum) Ethernet adapter; higher speeds are recommended
Other	Server must be dedicated to running NSM. NSM should not be installed on virtual systems such as VMWare and Microsoft VM Server due to high system I/O requirements.

Table 7 on page 6 describes the minimum requirements that must be met for each server when the GUI server and Device server are installed on separate servers.

Table 7: Minimum System Requirements—Management System on Separate Servers

Component	Minimum Requirements
Operating System	Solaris 10 operating system with End User Solaris Software Group package, or RHEL 32-bit ES/AS 4.0-Update 8 or 32-bit ES/AS 5.0-Update 4 (Minimal and Full Install) RHEL 32-bit ES 6.5 NOTE: Both servers must be running the same operating system version. For example, you cannot run the GUI server on a server running Linux, and the Device server on a server running Solaris.
CPU	Only Sun Microsystems UltraSPARC III 1GHz (or higher), OR Linux 2 GHz (x86) processor (or higher)
RAM	4 GB
Swap Space	2GB for the GUI server, 2 GB for the Device server
Storage	Hard disk drive with 7200 RPM (minimum); 15,000 RPM (recommended); 40 GB disk space (minimum); 80 GB disk space (recommended) By directory: <ul style="list-style-type: none"> • <code>/usr</code>—7 GB minimum • <code>/var</code>—10 GB min • <code>/tmp</code>—2 GB minimum
Network Connection	100 Mbps (minimum) Ethernet adapter; higher speeds are recommended
Device Connection bandwidth to NSM	56 Kbps (minimum)

Table 7: Minimum System Requirements—Management System on Separate Servers (continued)

Component	Minimum Requirements
Other	Each server must be dedicated to running NSM. NSM should not be installed on a virtual system such as VMWare and Microsoft VM Server due to high system I/O requirements.



NOTE: You can extend system performance and data capacity by expanding the minimum requirements specified for each component. See [“Hardware Recommendations” on page 283](#) for more information about the hardware and software appropriate for your specific network.

System Requirements—User Interface

Table 8 on page 7 describes the minimum system requirements that must be met for the User Interface.

Table 8: Minimum System Requirements—User Interface

Component	Minimum Requirement
Software	Microsoft Windows Vista, or Microsoft Windows XP, or RHEL 32-bit ES 4.0 or 32-bit ES 5.0, RHEL 32-bit AS 4.0 or RHEL 32-bit AS 5.0 (Minimal and Full Install) US English versions, or NSM supports installation of the NSM client on the Windows 7 32-bit and 64-bit operating system. However, before installing the client or updating to the latest schema, make sure that Active Windows 7 user should have enough read/write permission for creating new directories and read, write, and execute permission for creation and saving of new files under NSM_Installed_Directory . By default, NSM client is installed under program files (x86) on Windows 7 where permissions are usually restrictive. If the active Windows 7 user does not have permissions as mentioned above under program files(x86) , install NSM client under any other directory where sufficient read, write, and execute permission is provided for the directories and files. For example: C:/Users/Public .

Table 8: Minimum System Requirements—User Interface (continued)

Component	Minimum Requirement
Hardware	<p>IBM compatible PC</p> <p>Pentium 4 or equivalent</p> <p>RAM: 4 GB. For managing large scale setups (for example, with more than 1000 devices on the NSM server), Juniper recommends a minimum of 4 GB RAM.</p> <p>384 Kbps (DSL) or LAN connection — minimum bandwidth required to connect to the NSM management system.</p>

Choosing Standalone, Distributed, or High Availability Configurations

The two most important installation considerations are:

- Scale — The size of the network.

The NSM management system is designed to scale from the management of a few devices to huge networks of up to 3000 devices. For smaller networks, you can install the entire system on a single Linux or Solaris server. For larger networks, you can distribute the NSM management system by installing the Device server and GUI server on separate machines, and by using external shared disk systems.

- Failure tolerance — The effect on the organization upon failure of an NSM component and the downtime during repair.

You can increase fault tolerance by installing a standby management system on a single server for smaller installations, or on distributed servers for larger installations.

Some of the factors to consider include, but are not limited to:

- Number of devices managed
- Size of devices managed (for example, a NetScreen 5200 firewall/VPN system might have a larger impact than a NetScreen 5GT firewall appliance)
- Impact on the organization to temporary loss of logs during server failure (if not using multiple Device Servers the logs from firewalls would be lost until the single server is repaired)
- Amount of log data stored (this is a combination of the number of logs per day sent from the devices and the number of days the logs are required to remain on the management system)
- Customer's Linux/Solaris knowledge/skills
- Industry regulations governing the customer that might dictate the efforts they must go to in order to protect continuous log collection
- Main reason for using NSM (for example, firewall configuration only with occasional logging; heavy logging)

- Budget
- Future expansion of firewall network (future proofing)

For more information about recommended hardware for various types of networks, see [“Hardware Recommendations” on page 283](#).

You can design and implement NSM to scale to small, medium, and large enterprises, as well as service provider deployments. There are four main options for configuring NSM:

- [Standalone Configuration on page 9](#)
- [Distributed Configuration on page 9](#)
- [Simple High Availability Configuration on page 9](#)
- [Extended High Availability Configuration on page 10](#)

Standalone Configuration

The most straightforward implementation of the NSM management system is to install both components of the management system—GUI server and Device server—on the same server. This configuration is appropriate for most small firewall networks (recommended for no more than 100 devices, considerably less for networks containing large firewalls). It has the advantage of low cost and simplicity. Local backup for disaster recovery and external data storage are options for this configuration.

The NSM appliances can run as standalone configurations. See the *NSMXpress and NSM3000 User Guide* for details.

Distributed Configuration

For large enterprise networks that generate and store many traffic logs, we recommend that you install the GUI server and Device server on separate servers. The distributed system enables greater processing power per service. In addition, a failure of the GUI server would not result in the loss of log information as the Device server can continue to communicate with firewalls. You can also tailor the choice of hardware to the needs of each service (typically large RAM for GUI server and large disk capacity for the Device server).

Simple High Availability Configuration

You can also install and configure the management system to provide for high availability. This configuration option is recommended to minimize the impact of unplanned server outages.

To implement the management system for high availability, you need to install two physical servers: a primary server that runs on a server machine in active mode; and a secondary server that runs on a different server machine in standby mode. Upon the failure of any service on the primary server (or a hardware fault which results in the same effect) would cause both the GUI server and Device server to fail over to the standby server. The added benefit is automatic recovery of management service resulting in fewer lost firewall logs and reduced administrative down time. Note that the device logs would not be replicated to the peer server (only the config database).

During the installation or upgrade process, the NSM installer prompts you to specify whether or not you want the current server machine to participate in an HA cluster. If you choose to do so, the NSM installer prompts you to configure additional parameters enabling the high availability features on the management system.



NOTE: The NSM appliances can run in a simple high-availability configuration for fault tolerance.

Extended High Availability Configuration

The extended high availability configuration is the most extensive and complex configuration but has the greatest protection against component failure. A failure of the primary Device server would cause failover to the standby Device server. This new Device server would attempt connection with the primary GUI server. Failure of a GUI server would also cause failover to the standby GUI server. The current Device server would attempt to connect to the standby GUI server after a timeout period. In this configuration the failure of a single component has minimal impact on the system as a whole. In addition, the distributed system gives each service more system resource.

For more information about installing the management system for high availability, see [“High Availability Overview” on page 79](#).

Other Configuration Options

In addition to scale and fault tolerance, other configuration options include:

Local/Remote Database Backup

You can also configure the management system to perform an automatic backup of the GUI server database to the local server machine and, if necessary, to a remote server machine.



NOTE: You cannot perform backups to a remote server without also configuring the management system to perform backups to the local server.

During the installation or upgrade process, the NSM installer prompts you to specify whether this server machine requires local database backups. If you choose to do so, the NSM installer prompts you to configure the following additional parameters enabling the management system to perform automatic daily backups of the database:

- Hour of Day to store the database backup
- Number of database backups to keep
- Directory where local database backups are stored
- Full path to the **rsync** command—the management system uses the rsync utility to perform the database backup



NOTE: The NSM appliances are preconfigured to perform local database backups. See the *NSMXpress and NSM3000 User Guide* for details.

If you want to send copies of the file backups to a remote machine, the NSM installer prompts you to configure the IP Address of the remote machine



NOTE: If you want the management system to perform remote file backups, you will need to setup a trust relationship between the management system server and the remote machine.

NetScreen-Statistical Report Server Interoperability

If you are installing NetScreen-Statistical Report Server, you must configure it to work with NSM. During the installation or upgrade process, the NSM installer prompts you to configure parameters enabling the management system to communicate with the Statistical Report Server database and web server. If you choose to do so, the NSM installer prompts you to configure the following additional parameters enabling the management system to work with the NetScreen-Statistical Report Server database:

- Database type
- Database server IP address
- Database port
- Database name
- Database username
- Database password

You must restart the NSM GUI server process after installing NetScreen-Statistical Server to begin gathering statistics about managed devices.

Refer to the *NetScreen-Statistical Report Server Installer's Guide* for more information.



NOTE: The Netscreen-Statistical Report Server must be installed on a separate server from the NSM Servers.

Device Server Database

The NSM installer also prompts you to configure the additional parameters enabling the management system to work with a PostgreSQL Database used for the Device server. This database stores data related to the Profiler in NSM. You must specify a port number, superuser name and password. By default, the PostgreSQL Database uses port 5432; the superuser is "nsm".



NOTE: If you specify a username that does not already exist, the NSM installer creates the user for you. In this case, the NSM installer prompts you to create a password for the user. This password will not expire.



NOTE: The NSM appliance settings for PostgreSQL are preconfigured.

Next Steps

This chapter has provided you with the following:

- Overview of the NSM installation process
- Description of the contents in the NSM installation package
- Minimum system requirements to help you identify the appropriate hardware and software to install and run NSM
- Options for implementing components of the NSM management system to provide for enhanced performance, scalability, and high availability

Use this information to help you implement NSM and integrate it into your network. When you are ready to install NSM, there are four main options for configuring the management system depending upon the size and requirements of your specific network: Standalone, Distributed, Simple HA, or Extended HA configuration.

- [“Installing NSM in a Standalone Configuration” on page 15](#)—Includes specific information describing how to install and run the management system on the same server.
- [“Installing NSM in a Distributed Configuration” on page 49](#)—Includes specific information describing how to install and run the GUI server and Device server on separate servers. This configuration option enables you to extend performance and scalability for large enterprises.
- [“Installing NSM with High Availability” on page 79](#)—Includes specific information describing how to install and run the GUI server and Device server on the same server with HA (simple high availability configuration) or separate servers with HA (extended high availability configuration). This configuration option enables you to configure a primary and secondary management system that is highly available.
- [“Upgrading to NSM 2012.2 from an Earlier Version” on page 145](#)— Includes specific information describing how to upgrade previous installations of NSM to this version.
- [“Maintaining NSM” on page 251](#)— Includes specific information describing how to maintain, control, backup/restore, and uninstall the management system and User Interface.

For installation instructions for the NSM appliances, see the *NSMXpress and NSM3000 User Guide*.



NOTE: Juniper Networks devices require a license to activate the feature. To understand more about NSM Licenses, see, [Licenses for Network Management](#). Please refer to the Licensing Guide for general information about License Management.

CHAPTER 2

Installing NSM in a Standalone Configuration

After you decide how you want to deploy Network and Security Manager (NSM) in your network and you have identified and procured the appropriate hardware, you are ready to begin the installation process.

This chapter describes how to install the NSM management system for most typical cases: GUI server and Device server on the same server. These procedures include performing any prerequisite steps, running the management system installer, running the User Interface installer on your Windows or Linux client, and validating that you have installed the management system successfully.



NOTE: The NSM appliance uses a simplified installation procedure. See the *NSMXpress and NSM3000 User Guide* for details.



NOTE: Juniper Networks devices require a license to activate the feature. To understand more about NSM Licenses, see, [Licenses for Network Management](#). Please refer to the Licensing Guide for general information about License Management.

This chapter contains the following sections:

- [Suggested Standalone Configuration Installation Order on page 15](#)
- [Defining System Parameters on page 16](#)
- [Prerequisite Steps on page 19](#)
- [Installing NSM 2012.2 on page 24](#)
- [Installing the User Interface on page 39](#)
- [Next Steps on page 47](#)

Suggested Standalone Configuration Installation Order

The following procedure summarizes the process for installing NSM for most typical cases:

1. Define system parameters that you need to provide during the installation process.
2. Perform prerequisite steps.
3. Download the management system and user interface installer software from the Juniper Networks website. Alternatively, you can download the user interface software from the GUI server on the HTTPS port, after the NSM GUI server has been installed.
4. Run the management system installer on the system where you want to install the management system. During installation, you will need to:
 - Install a license. Obtain a license from the Juniper License Management Server (LMS) if you will be managing more and 25 devices (see [\[Unresolved xref\]](#)).
 - Specify that you want to install both the GUI server and Device server.
 - Install and configure the local database backup option.

If you are installing the GUI server and Device server on separate systems, see [“Installing NSM in a Distributed Configuration” on page 49](#) for more information.
5. Install the User Interface.
6. Launch the User Interface, then connect it to the management system.
7. Verify that you have successfully installed the management system and User Interface.

Defining System Parameters

During the installation process, you are required to configure common system parameters such as the location of the directories where you want to store data for the GUI server and Device server. We recommend that you define these system parameters before performing the management system installation.

[Table 9 on page 17](#) identifies the system parameters that you need to identify.

Table 9: Common System Parameters

Parameter	Description	Your Value
Device Server data directory	<p>Directory location on the Device server where device data is stored. Because the data on the Device server can grow to be large, consider placing this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the Device server stores data in:</p> <p>/var/netscreen/DevSvr/</p> <p>CAUTION: Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</p>	
GUI Server data directory	<p>Directory location on the GUI server where user data is stored. Because the data on the GUI server can grow to be large, consider placing this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI server stores data in:</p> <p>/var/netscreen/GuiSvr/</p> <p>CAUTION: Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</p>	
GUI server database log directory	<p>Directory location on the GUI server where database logs are stored. Because the data on the GUI server can grow to be large, consider placing this log data in another partition. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI server stores data in:</p> <p>/var/netscreen/GuiSvr/xdb/log</p>	
Management IP address	<p>The IP address used by the running GUI server.</p> <p>The default is the IP address of the machine that you are installing on.</p>	
https port	<p>The port number for listening for messages from the NSM API. The range is from 1025 through 65535. The default value is 8443.</p>	
Initial "super" user password	<p>The password required to authenticate the initial user in the system. By default, the initial superuser account receives all administrative privileges in the system.</p>	

Table 9: Common System Parameters (continued)

Parameter	Description	Your Value
One-time GUI server password	A password that authenticates the server to its peers in a high-availability configuration, or authenticates a regional server with a central manager.	
Configuration file management password	Configures a user and password for NSM to perform configuration file management operations, and a corresponding UNIX user and password. The NSM and UNIX passwords must be identical.	
Local database backup directory	<p>Directory location where local database backup data is stored.</p> <p>By default, the GUI server stores local database backup data at:</p> <p><code>/var/netscreen/dbbackup/</code></p>	
Path to the rsync utility executable	<p>Path to the rsync utility executable.</p> <p>The default path is:</p> <p><code>/usr/bin/rsync</code></p>	
Hour of the Day to Start Local Database Backup	<p>Time of day that you want the GUI server to backup the database. Type a two-digit number representing the time of day in a 24 hour clock notation (00 through 23). For example, if you want the backup to begin at 4:00 AM, type 04; if at 4:00 PM, type 16. We recommend that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI server completes the daily backup process within the hour specified every day.</p> <p>By default, the GUI server performs the daily backup within an hour after 2 AM.</p>	
Number of Local Database Backup Files Stored	<p>Total number of database backup files that the GUI server stores. When the GUI server reaches the maximum number of backup files you configure, it overwrites the oldest file.</p> <p>By default, the GUI server stores seven backup files.</p>	
Rsync Backup Timeout	Time value (in seconds) that the rsync utility waits before timing out backup operations. By default, the rsync utility waits 3600 seconds before timing out.	
Enable Logging	Enable logging related to local backup and HA.	
Device server Database Parameters	Parameters required for the Postgres Database used for the Device server. You must specify a port number, superuser name and password. By default, the Postgres Database uses port 5432; the superuser is "nsm".	

Prerequisite Steps

Before you install the management system, you need to perform the following prerequisite steps:

1. Ensure that the NSM appliance is accessible through a Serial Console
2. Log in to the appliance as root.

If you are already logged in as a user other than root, then enter the following command to become root:

```
su
```

At the password prompt, enter the root password for the .



NOTE: Although the management system runs with nsm user permissions, you must have root user permissions to run the NSM installer.

3. Partition drives for sufficient disk space to accommodate your planned data requirements. Ensure that you have allocated a maximum amount of disk space for the data partition (/ partition).

See [“Hardware Recommendations” on page 283](#) for more information about the disk space requirements appropriate for your specific network.

4. Run the system update utility for your appropriate platform to verify that you have all the prerequisite utilities and packages to run the NSM installer properly. See [“Running the System Update Utility” on page 20](#) for more information on running the system update utility.



NOTE: Some packages in the system update have specific version requirements, such as PostgreSQL. Be sure to use the packages distributed in the system update.

5. Configure shared memory size on your appropriate platform. See [“Configuring Shared Memory Size” on page 20](#) for more information.
6. If you plan to send copies of your file backups to a remote machine, then you must establish a trust relationship between the management system server and the remote machine. See [“Establishing a Trust Relationship” on page 21](#) for more information.
7. If you are installing NSM on a Solaris server, ensure that all required locales have been installed and that the necessary edits to the `/etc/default/init` files have been made. See [“Preparing a Solaris Server for NSM” on page 23](#) for details.
8. If you plan to manage more than 25 devices, you must obtain a license key file from the Juniper License Management Server (LMS) and install that file on the NSM Server or the NSM appliance. See [\[Unresolved xref\]](#).

Running the System Update Utility

Use the system update utility to upgrade your system with the latest patches and packages required to run the NSM management system installer properly.

To run the system update utility:

1. Copy the system update utility appropriate for your platform from the NSM Installation package directory to a suitable directory on the server.



NOTE: We recommend that you save the utility in the `/usr` subdirectory.

2. Uncompress the system update utility file using the **gzip** command. For example:

```
gzip -d nsm2012.2-systemupdate-linuxES_5.tar.gz
```

3. Uncompress the appropriate system update utility .tar file. For example:

```
tar xfv nsm2012.2-systemupdate-linuxES_5.tar
```

A subdirectory for the platform (for example, "es4", "es5", or "sol10") is created and all of the files required to update your system packages and utilities are extracted into that directory.

4. Navigate to the subdirectory.
5. Run the update shell archive script. For example, you can execute the shell archive script by running the following command:

```
<platform>.sh
```

For example, on Linux es4, the update script is named "rhes4_upd3.sh" and located in the directory "es4".

For Solaris, the **systemupdate-solaris *platform*.tar** file expands to *platform* and the update script is put in that directory. The script for Solaris is located in the same directory as the tar file. The name of the update script for Solaris is **update_solaris10.sh**.

The NSM installer proceeds to check your system for required updates. It next prompts you to press **Enter** to continue or **Ctrl-C** to stop.

6. Press **Enter** to continue. The NSM installer proceeds to cleanup the RPM database. Let the NSM installer run to completion. This process can take up to 20 minutes depending upon the number of packages that need to be installed.

Configuring Shared Memory Size

Both the GUI and Device server require that you modify the operating system shared memory in order to start and run.

On Solaris systems, you can do this by adding/updating the following in **/etc/system**:

```
set shmsys:shminfo_shmmax= 402653184
set shmsys:shminfo_shmmni=1
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256
set semsys:seminfo_semmmap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semml=32
```

On Linux systems, you can do this by adding/updating the following line in **/etc/sysctl.conf**:

```
kernel.shmmax= 402653184
```

After updating the shared memory requirements on your Linux or Solaris system, you must reboot the server for your new settings to take effect.

Establishing a Trust Relationship

If you want to send copies of your file backups to a remote machine, then you must establish a trust relationship between the management system server and the remote machine.

To establish a trust relationship between two machines:

1. Run the following commands on the management system server:

```
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
```

If prompted to enter a password, leave the value blank.

2. Run the following commands on the remote machine:

```
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
```

If prompted to enter a password, leave the value blank.

3. From the remote machine, copy **.ssh/id_rsa.pub** to the management system server's **.ssh/authorized_keys** directory. For example:

```
scp .ssh/id_rsa.pub root@<IP addr management system>:/root.ssh/authorized_keys
```

4. From the server running the management system, copy **.ssh/id_rsa.pub** to the remote machine's **.ssh/authorized_keys**. For example:

```
scp .ssh/id_rsa.pub root@<IP addr remote machine>:/root.ssh/authorized_keys
```



NOTE: If the remote machine already has established trust relationships with other computers, overwriting the `authorized_keys` file will break those trust relationships. Instead, copy the contents of the `id_rsa.pub` file onto a new line at the end of the `authorized_keys` file on the remote machine.

5. Test connectivity via SSH from the primary server to the remote machine and vice versa. For example, to test SSH connectivity from NSM Server1 to remote machine, enter the following command:

```
ssh root@<IP ADDRESS of remote machine>
```

6. Change the permissions of the `.ssh` directory on each machine to owner-only, using the following command:

```
chmod -r 0700 ~/.ssh
```

7. Validate that you do not receive a prompt to enter a password to access the remote machine.

If you do receive a password prompt, the remote database replication will not function properly, check for errors in the steps for establishing a trust relationship and repeat the process.

Establishing a Trust Relationship on a High Availability Cluster

To enable secure communication between the NSM devices operating in a high availability cluster mode, you must establish a trust relationship between the primary server and the secondary server devices.

To establish a trust relationship between two servers:

1. Enter `sudo su -` and the admin password to gain root access to the primary server.
2. Run the following commands on the primary server:

```
su nsm
```

```
cd /home/nsm
```

```
ssh-keygen -t rsa
```



NOTE: If you are prompted to enter a passphrase, leave the value blank.

3. From the primary server, manually copy the `.ssh/id_rsa.pub` public key to the secondary server and place it in `.ssh/authorized_keys`.

```
scp .ssh/id_rsa.pub admin@ <IP address of secondary server>
:/home/admin/authorized_keys
```

Repeat steps 1 through 3 on the secondary device.

4. On the secondary server, change user privileges to root by entering the following command at the prompt:

```
exit
```

5. Move the authorized_keys file that you copied to admin into nsm/.ssh.

```
mv /home/admin/authorized_keys /home/nsm/.ssh/authorized_keys
```

6. Change the ownership of the authorized_keys.

```
chown nsm:nsm /home/nsm/.ssh/authorized_keys
```

Repeat steps 4 through 6 on primary device.

7. Test connectivity through SSH from the primary server to the secondary server and NSM user privileges by using the following command:

```
ssh nsm@<IP address of secondary server>
```

If you do not receive a prompt to enter a password, a trust relationship between two machines is established.

If you do receive a password prompt, verify the ownership of the `/home/nsm/.ssh` directory and the `/home/nsm/.ssh/authorized_keys` file. They should be `nsm:nsm`. Repeat the above steps if you continue to receive a password prompt.

8. Test connectivity through SSH from the secondary server to the primary server with nsm user privileges by using the following command:

```
ssh nsm@<IP address of primary server>
```

Preparing a Solaris Server for NSM

Perform these steps if you plan to install NSM on a Solaris 10 server:

1. Install required locale files.

Use the following command to check which locale files are currently installed:

```
/usr/bin/locale -a
```

Ensure that the following locales are installed. If you have all required locales, proceed to Step 2.

```
C
POSIX
en_CA
```

```
en_CA.IS08859-1
en_CA.UTF-8
en_US
en_US.IS08859-1
en_US.IS08859-15
en_US.IS08859-15@euro
en_US.UTF-8
es
es.UTF-8
es_MX
es_MX.IS08859-1
es_MX.UTF-8
fr
fr.UTF-8
fr_CA
fr_CA.IS08859-1
fr_CA.UTF-8
iso_8859_1
```

Use the Solaris 10 installation DVD to load any missing locales. The minimum supported Solaris 10 revision is 6/06. You can download the DVD from www.sun.com. Mount the DVD (in this example, `/solaris`) and issue the following commands:

```
/usr/sbin/pkgadd -d /solaris/Solaris_10/Product SUNWladm
```

```
/usr/sbin/localeadm -a en_US -d /solaris/Solaris_10/Product
```

2. Edit the `/etc/default/init` file to include the following lines:

```
LC_COLLATE=en_US.UTF-8
LC_CTYPE=en_US.UTF-8
LC_MESSAGES=C
LC_MONETARY=en_US.UTF-8
LC_NUMERIC=en_US.UTF-8
LC_TIME=en_US.UTF-8
```

3. Reboot the Solaris server.

```
/usr/sbin/reboot
```

Installing NSM 2012.2

The NSM installer is designed to guide you through all of the steps to configure the required system parameters.

To install the management system on the same system:

1. Load the NSM installer software onto the server where you have decided to use NSM 2012.2. You can download the NSM installer from the [Juniper Networks website](#).
2. Navigate to the directory where you saved the management system installer file. We recommend that you save the NSM installer in the `/var/tmp` subdirectory.

3. Run the management system installer.

On Linux, run the following command:

```
sh nsm2012.2_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2012.2_servers_sol_sparc.sh
```

The installation begins automatically by performing a series of pre installation checks. The NSM installer ensures that:

- The OS version and specified architecture are compatible.
- You are installing the correct software for your operating system.
- All of the needed software binaries and packages are present.

If any component is missing, the NSM installer displays a message identifying the missing component:

```
Checking for platform-specific packages.....FAILED
The Following list of Packages are Required for NSM installation.
Please install the system update utility before continuing.
chkfontpath
```

- You have the correct version of the PostgreSQL database.
- You have correctly logged in as root and that the NSM user exists. The NSM installer creates the NSM user, if it does not already exist.
- For Linux servers, the NSM installer checks whether iptables is running. If not, then the NSM installer continues.

If iptables is running, the NSM installer displays a message similar to the following:

```
Checking for iptables service.....ok
Iptables is found to be running on the system. Please make sure the ports
7801 7802, 443, 7800, 7804 are open and available for NSM to run.

Please press enter to continue:
```

Ensure the required ports for NSM are available before continuing.

- The system has sufficient disk space and RAM.

The NSM installer stops any running servers.



NOTE: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the NSM installer successfully performed a task.
- “OK” indicates that the NSM installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the NSM installer performed a task or check, but it was unsuccessful. See the install log for information about the failure. This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of the install, the log might be in `/var/tmp`.

The NSM installer extracts the software payloads and prompts you to install NSM with the base license.

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 3
```

4. The NSM installer prompts you to specify the components that you want to install. Enter **3** to specify that you want to install both the GUI server and the Device server.



NOTE: If you have installed a previous version of the management system, you might see different menu options.

```
Do you want to do NSM installation with base license? (y/n) [y]>
Enter base directory location for management servers [/usr/netscreen]>
```

5. For a base license installation—that is, one that does not require the license key file—enter **y**.

For an installation that requires a license key file, enter **n**. You enter the license file path later. See [\[Unresolved xref\]](#) for information about obtaining license keys.

6. The NSM installer prompts you to specify a base directory in which to install the management server files.

Press Enter to accept the default **/usr/netscreen** directory, or type the full path name to a directory and then press Enter.

The NSM installer prompts whether you want to enable FIPS support.

7. If you require FIPS support, enter **y**. Otherwise, press Enter to accept the default value.

What happens next depends on whether you selected to install with a base license or with a license key file. If you are installing with a base license, skip step 8.

8. If you chose to install a license key file, NSM installer displays the installation ID of the system and prompts you to enter the license key file path.

```
The installation ID for this system is: 3FFFEA90278AA
```

```
Enter the License File Path>
```

- a. Use the installation ID to obtain a license key file from the LMS system and save it on your local drive as described in [\[Unresolved xref\]](#).
- b. Enter the license key file path.

The NSM installer validates the license key file.



NOTE: If the NSM installer prompts for license file and no license is available, press Ctrl-Z to exit NSM installer.

The NSM installer prompts you to determine if you want this server to participate in an HA cluster.

9. Enter **n** if you do not want the server to participate in an HA cluster. If you are planning to configure the management system with HA enabled, enter **y**. See [“Introduction” on page 3](#) for more information, and then turn to [“Installing NSM with High Availability” on page 79](#), and follow the instructions there.

The NSM installer prompts you to specify a location to store the NSM data files.

10. Set the directory location for storing the management system data files:

- a. Type the directory location for storing the Device server data files or press Enter to accept the default location `/var/netscreen/DevSvr`.

The NSM installer prompts you to specify a location for storing the GUI server data files.

- b. Type the directory location for storing the GUI server data files or press Enter to accept the default location `/var/netscreen/GuiSvr`.
- c. Type the directory location for storing the database files for the GUI server or press Enter to accept the default location `/var/netscreen/GuiSvr/xdb/log`.



NOTE: You cannot store files in an existing directory location. This feature safeguards against overwriting any existing data. If you specify an existing directory, NSM installer prompts you to try again.

The NSM installer next prompts you to specify the management IP address for the server.

11. Type the management IP address for the server. This address should be the same IP address as the server that you are installing on. The NSM installer sets the IP address and port number on the GUI server enabling the Device server to connect. The Device server attempts to connect to the GUI server using port 7800 by default.
12. Enter a port number for listening for messages from the NSM API. The default value is 8443. This parameter must be between 1025 and 65535.

The NSM installer prompts you to type a password for the superuser account. The initial administrator or superuser account is the account that you use when you first log in to NSM using the NSM user interface (UI). This account authenticates communication between the management system and the NSM UI. It possesses all administrative privileges by default.

13. Type any text string longer than eight characters for the password. Type the password again for verification.



NOTE: Make a note of the password that you have set for the superuser account. You need this when you first log in to the UI.

14. Enter a one-time password for the GUI server. This password authenticates this server to its peers in a high-availability configuration and to the central manager.

The NSM installer prompts you to determine if you want to use a Statistical Report Server with the GUI server.

15. Enter **n** if you are not installing NetScreen-Statistical Report Server with NSM. Enter **y** if you are installing NetScreen-Statistical Report Server with NSM.

If you typed **y**, NSM installer prompts you to configure parameters required for the management system to work with the Statistical Report Server (that is, database type, database server IP address, database port, database name, database username,

database password). Refer to the *NetScreen-Statistical Report Server Installer's Guide* for more information about these parameters.

The NSM installer next creates a user in the NSM group for performing configuration file management actions and prompts for a password.

16. Enter a password for the configuration-file management (CFM) user.

Because the UNIX password can not be saved in plain text format, NSM installer prompts a second time to enter the same password to save in `guiSvr.cfg` file, which will be used for auto archival configuration settings.



NOTE: The CFM passwords for NSM and for UNIX must be identical, although NSM does not check that they are the same.

The NSM installer next prompts if you want the server processes to be restarted automatically on failure.

17. Enter **y** to have the server processes restarted automatically on failure.

The NSM installer next prompts if you want this server to perform a daily backup of the database locally.

18. Enter **y** if you want NSM to perform a local backup of the database on a daily basis. Enter **n** if you do not want the management system to backup the database locally.

If you specify that you want to perform automatic backups, NSM installer prompts you to configure options for the backup operation:



NOTE: If you want to specify remote backup, you must allow local backup.

- a. Enter a two-digit number (00 through 23) to specify the hour of day that you want the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, type **12**; for midnight, type **00**. Press Enter to accept the default setting of 02 (2:00 AM).
- b. Enter **n** to specify that you do not want daily backups to be sent to a remote server. If you enter **y**, NSM installer prompts you to enter an IP address for the remote backup server.



NOTE: If you want to perform backups to a remote server, make sure to establish a trust relationship with that server. See [“Establishing a Trust Relationship” on page 21](#).

- c. Enter a number (from 0 to 7) to specify how many database backup files NSM stores. After the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press Enter to accept the default setting of seven backup files. By default, the management system stores backup files in `/var/netscreen/dbbackup`.

- d. Type a number specifying how many seconds you want NSM to wait while performing backups until the process times out.
- e. Designate a directory location for locally storing the NSM database backup. Press Enter to accept the default location **/var/netscreen/dbbackup**.

The NSM installer prompts you to configure the Device server database.

19. Configure the Device server database as follows:

- a. Enter a port number for the Device server database.
- b. Enter a name for the database superuser. If you specify a user that does not already exist, NSM installer prompts you for a password. Enter the password again for verification.

The NSM installer prompts you to start servers after installation is complete.

20. If you want to start the GUI and Device servers after the installation has finished, enter **y**. The NSM installer will start the server processes with NSM user permissions.

Enter **n** if you do not want to start the servers.

The NSM installer prompts you to verify your installation configuration settings.

21. Verify your settings. If the configuration settings are correct, enter **y** to proceed. If you enter **n**, NSM installer returns to the previous prompt.

The NSM installer performs the following actions:

- Installs the Device server.
- Installs the GUI server.
- Installs the HA server.
- Performs post installation tasks.

Several messages display to confirm the installation progress.

The installer generates a log file with the output of the installation commands for troubleshooting purposes. The naming convention used for the installation log file is:

```
netmgtInstallLog.<current date><current time>
```

For example if you ran NSM installer on December 1, 2003 at 6:00 PM, the installation log file would be named:

```
netmgtInstallLog.20031201180000
```

After the installation finishes, it indicates the name of the installation log file and the directory location where it is saved.



NOTE: If the installation fails to install NSM, the installation log file will be in `/var/tmp`.

The NSM installer runs for several minutes, and then returns you to the command prompt.



NOTE: If you are installing NSM for the first time on a Solaris server, you must reboot the server after installation.

Typical Output for a Standalone Installation

An example of the output for a typical standalone installation is as follows:

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 3

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]>
```

DEVICE SERVER SETUP DETAILS

The Device Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/DevSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition.

Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

Enter data directory location [/var/netscreen/DevSvr]>

GUI SERVER SETUP DETAILS

The GUI Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/GuiSvr. Because the user data (including database data and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition.

Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

Enter data directory location [/var/netscreen/GuiSvr]>

The GUI Server stores all of the database logs under a single directory. By default, this directory is /var/netscreen/GuiSvr/xdm/log. Because the database log can grow to be quite large, it is sometimes desirable to place this log in another partition.

Please enter an alternative location for this log if so desired, or press ENTER for the location specified in the brackets.

Enter database log directory location [/var/netscreen/GuiSvr/xdm/log]>

Enter the management IP address of this server [10.157.48.108]>

Enter the https port for NBI service [8443]>

Setting GUI Server address and port to 10.157.48.108:7801 for Device Server

Please enter a password for the 'super' user

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

Enter the one-time password for this Gui Server

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

CFM password for user 'cfmuser'

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

Enter the same password again for CFM user

```

Changing password for user cfmuser.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Will server processes need to be restarted automatically in case of a failure?
(y/n) [y]>

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

Enter database backup directory [/var/netscreen/dbbackup]>

##### DEVSVR DB SETUP DETAILS #####

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

##### POST-INSTALLATION OPTIONS #####

Start server(s) when finished? (y/n) [y]> y

##### CONFIRMATION #####

About to proceed with the following actions:
- Install Device Server
- Install GUI Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine will have base license with maximum 25 devices
- This machine does not participate in an HA cluster
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdm/log
- Use IP address 10.157.48.108 for management
- Use port 8443 for NBI Service
- Connect to GUI Server at 10.157.48.108:7801
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- Servers will be restarted automatically in case of a failure
- Local database backups are enabled

```

```
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start server(s) when finished: Yes

Are the above actions correct? (y/n)> y

##### PERFORMING INSTALLATION TASKS #####

----- INSTALLING Device Server -----
Looking for existing RPM package.....ok
Removing existing Device Server RPM.....ok
Installing Device Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in Device Server config file(s).....ok
Setting permissions for Device Server.....ok
----- Setting up PostgreSQL for DevSvr -----
Setting up PostgreSQL for DevSvr.....ok
Installation of Device Server complete.

----- INSTALLING GUI Server -----
Looking for existing RPM package.....ok
Removing existing GUI Server RPM.....ok
Installing GUI Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in GUI Server config file(s).....ok
Setting permissions for GUI Server.....ok
Running generateMPK utility.....ok
Running fingerprintMPK utility.....ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Enabling Device Server start script.....ok
Enabling GUI Server start script.....ok
Enabling HA Server start script.....ok

##### PERFORMING POST-INSTALLATION TASKS #####
Running nacnCertGeneration.....ok
```

```

Running idpCertGeneration.....ok
Converting GuiSvr SetDB to XDB .....ok
Loading GuiSvr XDB data from init files .....ok
ok
Running webproxy Cert Generation.....ok
Removing staging directory.....ok
Starting GUI Server.....ok
Starting Device Server.....ok
Starting HA Server.....ok

NOTES:
- Installation log is stored in
/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20080902134533

- This is the GUI Server fingerprint:
14:7C:3A:AD:F9:96:9A:80:7B:0B:D7:49:DE:CC:91:B8:4F:42:77:42
You will need this for verification purposes when logging into the GUI
Server. Please make a note of it.

[root@C73-16 ~]#

```

Installing NSM with an IPv6 Management Address

Beginning in NSM2012.2R10, NSM can be installed with an IPv6 management address for a standalone installation.



NOTE: You must configure the IPv6 address in the NSM server before starting the installation.

Typical Output for a Standalone Installation

An example of the output for a typical standalone IPv6 installation is as follows:

```

[root@nsm-b3-vm7 ~]# sh nsm2012.2R10_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
WARNING:
Please make sure the following lines are present in the /etc/sysctl.conf file.
kernel.shmmax= 402653184
The install will exit if they aren't present. Please Reboot the system before
continuing
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok

```

```
Checking if selinux is enabled.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 3

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

Select Device Schema to be loaded in NSM

1) Load all Device Family Schemas
2) Load Screen OS Device Schema only (Screen OS)
3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
Enter selection (1-3)[1]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]>

##### DEVICE SERVER SETUP DETAILS #####

The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

##### GUI SERVER SETUP DETAILS #####

The GUI Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/GuiSvr. Because
the user data (including database data and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/GuiSvr]>
```

```

The GUI Server stores all of the database logs under a single directory.
By default, this directory is /var/netscreen/GuiSvr/xdb/log. Because
the database log can grow to be quite
large, it is sometimes desirable to place this log in another
partition.
Please enter an alternative location for this log if
so desired, or press ENTER for the location specified in the
brackets.
Enter database log directory location [/var/netscreen/GuiSvr/xdb/log]>

Enter the type of management IP address of this server (4-IPv4 / 6-IPv6) [4]> 6
Enter the management IPv6 address of this server [fc00::10:205:1:95]>

Enter the https port for NBI service [8443]>

Setting GUI Server address and port to fc00::10:205:1:95:7801 for Device Server

Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter the one-time password for this Gui Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

CFM password for user 'cfmuser'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>
Enter the same password again for CFM user
Changing password for user cfmuser.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Will server processes need to be restarted automatically in case of a failure?
(y/n) [y]> n

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]> y

Enter the type of IP address for remote backup machine (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address of the remote backup machine []> fc00::10:205:1:97

Enter number of database backups to keep [7]>

```

```

Enter the rsync backup timeout [3600]>

Enter database backup directory [/var/netscreen/dbbackup]>

The database backup server(s) requires that you have previously installed the ssh
program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between this machine and the
remote machine, via ssh-keygen, is a requirement for the
remote replication to work properly.
Please reset the trust relationship with 'nsm' user.
Here are sample commands:
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

##### DEVSVR DB SETUP DETAILS #####

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

##### POST-INSTALLATION OPTIONS #####

Start server(s) when finished? (y/n) []> y

##### CONFIRMATION #####

About to proceed with the following actions:
- Install Device Server
- Install GUI Server
- Install High Availability Server
- This machine will have base license with maximum 25 devices
- Store base directory for management servers as /usr/netscreen
- All Device Families Schemas Load
- This machine does not participate in an HA cluster
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdm/log
- Use IP address fc00::10:205:1:95 for management
- Use port 8443 for NBI Service
- Connect to GUI Server at fc00::10:205:1:95:7801
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- Servers will not be restarted automatically
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: fc00::10:205:1:97

```

```
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Path for the ssh command: /usr/bin/ssh
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start server(s) when finished: Yes
```

```
Are the above actions correct? (y/n)> y
```

Starting Server Processes Manually

If you did not specify the NSM installer to start the servers when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually, run the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

The HA Server process automatically starts the GUI server and Device server processes.



NOTE: NSM server processes always run with NSM user permissions, even if you have root user permissions when you start them.

Validating Management System Status

To validate that the management system is started and running properly, we recommend that you view the status of all the running server processes (the HA, Device, and GUI Servers) to confirm that all services are running.

See [“Controlling the Management System” on page 251](#) for more information on manual commands that you can send to the HA Server, Device server, and GUI server.

Installing the User Interface

The NSM user interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based that meets minimum system requirements. See [“System Requirements—User Interface” on page 7](#) for more information on the minimum system requirements for the UI.

The InstallAnywhere wizard guides you through all of the steps required to configure and install the NSM UI. After you install the UI, you can connect it to the management system.



NOTE: If you are running winrunner software with Java plugins on your client machine, ensure that those plugins are JRE version 1.6 or later.



NOTE: If you are installing the UI on RHEL 5, first install the “libXp” package. You can obtain libXp from RedHat.

We recommend that you exit all running applications before installing the UI.

To install the NSM UI:

1. Log in as an Administrator user on the where you are installing the UI.



NOTE: For instructions on adding users to the Administrator group, refer to your operating system manual.

2. Download the UI installer from the [Juniper Networks web site](#) to the where you are installing the UI.



NOTE:

You can also download the UI installer using the following method:

1. Go to <https://<GUI-Server-IP-Address>:8443> using the IPv4 or IPv6 management address that is assigned to the GUI server. For example:
 - <https://192.168.1.1:8443> for IPv4 management address
 - [https://\[2000::ffff:192:168:1:1\]:8443](https://[2000::ffff:192:168:1:1]:8443) for IPv6 management address



NOTE: While downloading the NSM client, you can ignore the self-signed certificate error.

2. To download the UI on a Windows-based PC or a Linux-based PC, click **Windows UI Client** or **Linux UI Client**, respectively.

3. Run the UI installer.

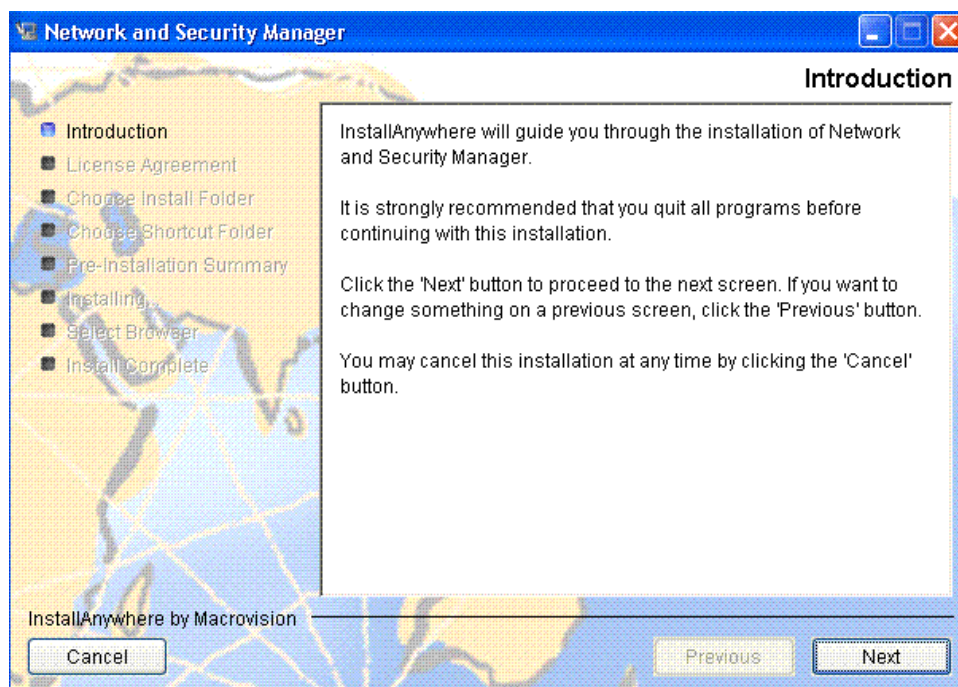
If you are installing the UI on a Windows-based PC, then double-click on the NSM installer executable.

If you are installing the UI on a Linux-based , then launch it from a command line using the following command:

```
sh nsm2012.2_ui_linux_x86.bin
```

An Introduction screen for the Install Anywhere wizard appears similar to [Figure 1 on page 41](#).

Figure 1: UI Installer Introduction Screen



Click **Next** to continue the installation. The License Agreement screen appears.

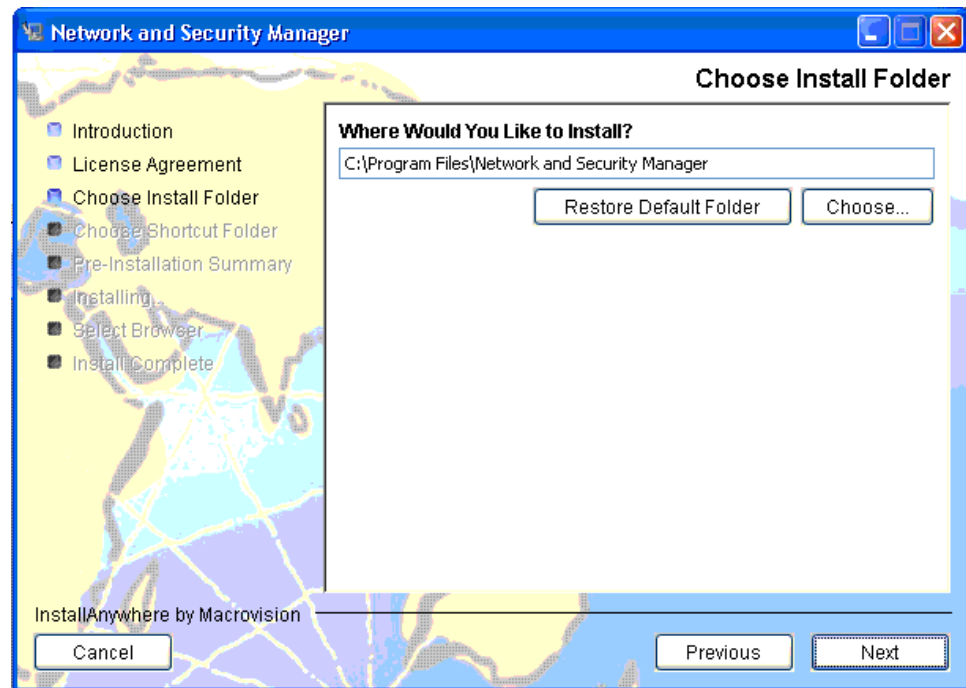
4. Review the License Agreement carefully. If you choose to accept the terms of the License Agreement, click the button next to the appropriate statement, and then click **Next** to continue.



NOTE: If you choose to not accept the terms of the License Agreement, then you are unable to proceed with the installation.

If you accepted the License Agreement, then the Choose Install Folder screen appears as shown in [Figure 2 on page 42](#).

Figure 2: UI Installation—Choose Install Folder



5. To accept the default install folder, click **Next**.

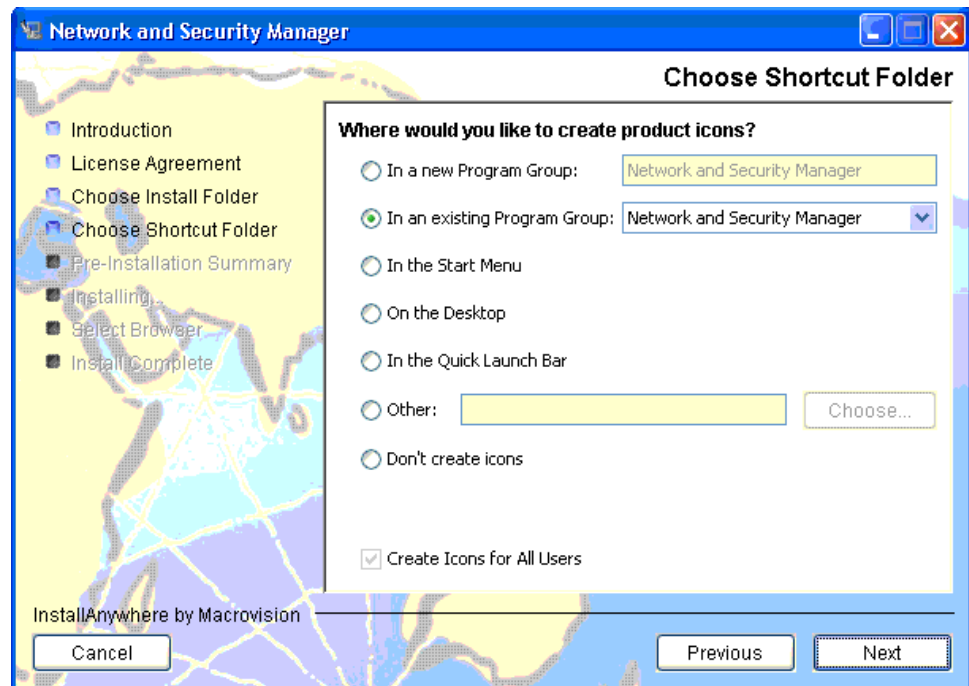


NOTE: If you are installing on a Windows-based , then NSM installer saves the UI software files in C:\Program Files\Network and Security Manager by default. If you are installing on a Linux-based , then NSM installer saves the UI software files in /install_user_homedir/Network and Security Manager by default.

To specify a new or different folder location, click **Choose**. If you decide to accept the default install folder, then click **Restore Default Folder**.

On Windows-based computers, the Choose Shortcut Folder screen appears as shown in [Figure 3 on page 43](#).

Figure 3: UI Installation—Choose Shortcut Folder



On Linux-based computers, the Choose Link Folder screen appears.

6. Select where you would like to create the NSM product icons. Or, if you are installing on a Linux-based , select where you would like to create links to the NSM UI program. Click **Next** to continue. The Pre-Installation Summary screen appears as shown in [Figure 4 on page 44](#).

Figure 4: UI Installation—Preinstallation Summary



7. Verify that the information is correct. To make a change to any of the previous configuration options, click **Previous**. When you are satisfied that the information is correct for this installation, click **Install**. The NSM installer proceeds to install the software files for the UI.
8. If you do not have a default web browser configured, then the Select Browser screen appears. Click **Choose** to navigate to the subdirectory where your web browser software files are located. Click **Next** to continue. When the installation is complete, a screen indicating “Install Complete” appears.



NOTE: If you do not select a default web browser, then the UI is not able to launch the NSM online help. If you still want to use the online help, then you can configure your web browser using the Preferences menu from the UI.

9. Click **Done** to exit the installation program.

The installer generates a log file with information describing the context of the installation process. For troubleshooting purposes, you might need to access it. The installation log is saved by default in the following directory locations:

For Windows-based computers:

```
C:\Documents and Settings\<user name>\.nsm\
```

For Linux-based computers:

```
/<install_user_homedir>/ .nsm/
```



NOTE: The `.nsm` subdirectory is a hidden subdirectory on Linux systems.

The Installation log file is named: `_out.date/time stamp.dat`

Running the User Interface

After you have completed installing the UI, you can launch the application and verify that you can connect to the management system.

The first time you open the UI, you need to specify the host name (or IP address) of the management system that you want to connect to, a username, and password. The default username for new installations is “super”; the default password is the password you specified when configuring the management system. Passwords and usernames are case sensitive.

To log in to the UI for the first time:

1. Run the NSM UI.

If you are running the UI on a Windows-based PC, then double-click on the NSM icon.

If you are running the UI on a Linux-based , then launch it by double clicking on the NSM application icon (specify that you want to run the program) or launch it from a command line. From the command line, navigate to the subdirectory where you have installed the UI software files, and then launch the UI application by running the shell archive script provided. The Login window appears.

2. Verify that the username in the Login field provided is the initial admin user called “super”. If not, type **super** in the Login field.
3. In the password field, type the password that you specified when you installed the management system.
4. In the server field, type the IP address you assigned to the GUI server. If you have enabled DNS lookup, then type the host name instead of the IP address.



NOTE: If the NSM installation uses an IPv6 address, type the IPv6 address that is assigned to the GUI server.

5. Click **OK**.

The UI appears indicating that the installation was successful.

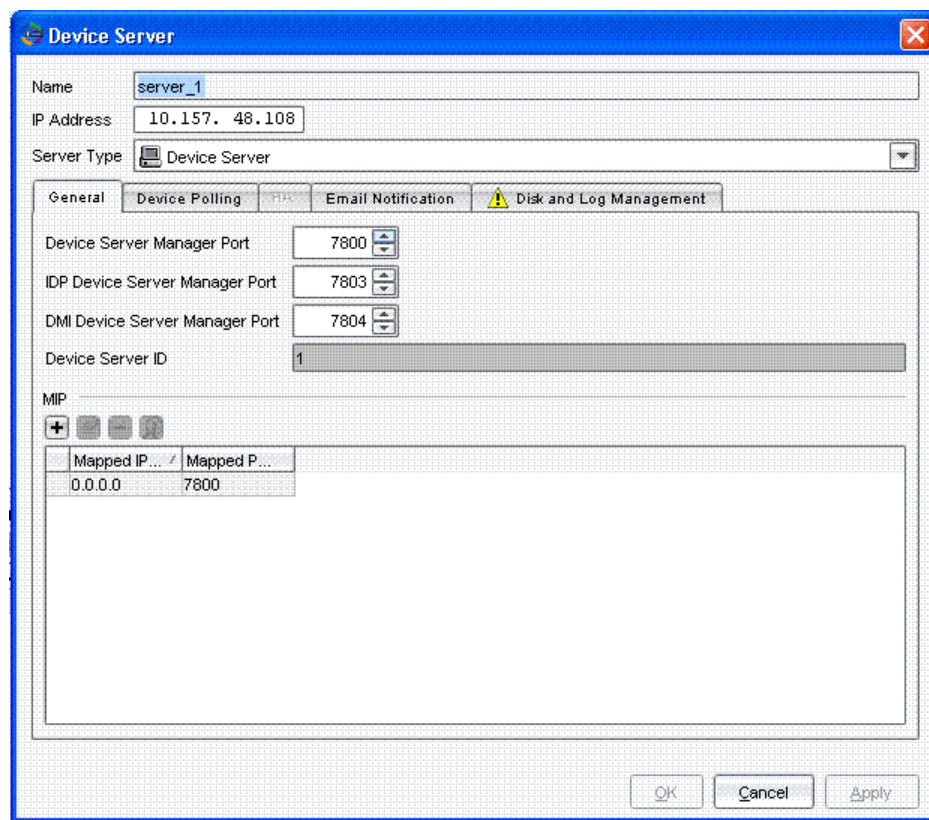
Validating the NSM Installation

After you have installed the management system and UI, We recommend that you validate basic information configured on the Device server. You can use the Server Manager to view and edit your configuration on the management system.

To validate your configuration on the Device server:

1. From the NSM UI Administrative panel, select **Server Manager>Servers**. The Servers view appears displaying Device server and GUI server information.
2. Click on the Device server, and then click on the Edit icon or right-click on the Device server and select **Edit** to view all information available on the Device server. A screen appears similar to [Figure 5 on page 46](#).

Figure 5: Validating the NSM Installation



3. Use the General tab to verify the following information:
 - Device Server Manager Port—The default port is 7800.
 - IDP Device Server Manager Port—The default port is 7803.
 - DMI Device Server Manager Port—The default port is 7804.

- Device Server ID—The ID number identifies the Device Server; you cannot change the Device Server ID.
- Mapped IP address—The IP address that is manually defined in the UI.



NOTE: You can configure the Device server to use a Mapped IP (MIP) address. A MIP maps the destination IP address in an IP packet header to another static IP address, enabling the managed device to receive incoming traffic at one IP address, and automatically forward that traffic to the mapped IP address. MIPs enable inbound traffic to reach private addresses in a zone that contains NAT mode interfaces.

4. Click **OK** when you are finished.

Running the User Interface in Demo Mode

Before you begin using NSM to configure and manage your network, we recommend that you first run the UI in Demo mode to get familiar with its features. Demo mode is an option in the UI enabling you to run the UI disconnected from the management system.

To run the UI in Demo mode:

1. Run the NSM UI. The Login window appears.
2. Type any username in the Login field provided.
3. Type any password in the Password field provided.
4. Select ***DEMO MODE*** from the Server field list.
5. Click **OK**. The user interface appears in demo mode.
6. Use the demo mode interface with the *Network and Security Manager Online Help* and the *Network and Security Manager Administration Guide* to gain familiarity with the interface.

Next Steps

Now that you have completed installation of the NSM management system and UI, you can begin to manage your network using NSM. Refer to the *Network and Security Manager Administration Guide* for information describing how to plan and implement NSM for your network. You can also refer to the *Network and Security Manager Online Help* for task specific information.

CHAPTER 3

Installing NSM in a Distributed Configuration

For larger enterprises, where you expect to generate a large amount of traffic logs, we recommend that you install the GUI server and Device server on separate servers.

This chapter describes how to install the Network and Security Manager (NSM) management system—GUI server and Device server—on separate servers. This installation includes performing any prerequisite steps, running the management system installer, running the User Interface installer, and validating that you have installed the management system successfully.

This chapter contains the following sections:

- [Suggested Distributed Configuration Installation Order on page 49](#)
- [Defining System Parameters on page 50](#)
- [Prerequisites on page 53](#)
- [Installing the GUI Server on page 53](#)
- [Installing the User Interface on page 62](#)
- [Adding the Device Server in the User Interface on page 63](#)
- [Installing the Device Server on page 63](#)
- [Installing NSM with an IPv6 Management Address on page 69](#)
- [Starting Server Processes Manually on page 78](#)
- [Validating Management System Status on page 78](#)
- [Next Steps on page 78](#)

Suggested Distributed Configuration Installation Order

The following procedure summarizes the process for installing the management system on separate servers:

1. Define system parameters that you need to provide during the installation process.
2. Perform prerequisite steps.

3. Download the management system and User Interface installer software from the [Juniper Networks website](#).
4. Run the management system installer on the server where you want to install the GUI server. During installation, you will need to:
 - Install a license. Obtain a license from the Juniper License Management Server (LMS) if you will be managing more and 25 devices (see [\[Unresolved xref\]](#))
 - Specify that you want to install the GUI server.
 - Install and configure the local database backup option (optional).
5. Install the User Interface.
6. Launch the User Interface, then connect it to the GUI server. Add and configure the Device server.
7. Run the management system installer on the server where you want to install the Device server. Specify that you want to install the Device server. Install and configure the local database backup option (optional).

You do not need to install a license for the Device server.
8. Transfer certificate files from the server that you are installing the Device server to the server that you are installing the GUI server.

Defining System Parameters

During the installation process, you are required to configure common system parameters such as directory locations to store data for the GUI server and Device server. We recommend that you define these system parameters before performing the management system installation.

[Table 10 on page 51](#) identifies the system parameters that you need to identify.

Table 10: Distributed Configuration—System Parameters

Parameter	Description	Your Value
Device Server data directory	<p>Directory location on the Device server where device data is stored. Because the data on the Device server can grow to be large, consider placing this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the Device server stores data in:</p> <p>/var/netscreen/DevSvr/</p> <p>CAUTION: Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</p>	
GUI Server data directory	<p>Directory location on the GUI server where user data is stored. Because the data on the GUI server can grow to be large, consider placing this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI server stores data in:</p> <p>/var/netscreen/GuiSvr/</p> <p>CAUTION: Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</p>	
GUI server database log directory	<p>Directory location on the GUI server where database logs are stored. Because the data on the GUI server can grow to be large, consider placing this log data in another partition. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI server stores data in:</p> <p>/var/netscreen/GuiSvr/xdb/log</p>	
Management IP address	<p>The IP address and port used by the running GUI server.</p> <p>The default is the IP address of the machine that you are installing on.</p>	
https port	<p>The port number for listening for messages from the NSM API. The range is from 1025 through 65535. The default value is 8443.</p>	
Initial “super” user password	<p>The password required to authenticate the initial user in the system. By default, the initial superuser account receives all administrative privileges in the system.</p>	

Table 10: Distributed Configuration—System Parameters (continued)

Parameter	Description	Your Value
One-time GUI server password	A password that authenticates the server to its peers in a high-availability configuration, or authenticates a regional server with a central manager.	
Configuration file management password	Configures a user and password for NSM to perform configuration file management operations, and a corresponding UNIX user and password. The NSM and UNIX passwords must be identical.	
Local Database Backup directory	<p>Directory location where local database backup data is stored.</p> <p>By default, the GUI server stores local database backup data at:</p> <p><code>/var/netscreen/dbbackup/</code></p>	
Path to the rsync utility executable file	<p>Path to the rsync utility executable file.</p> <p>The default path is:</p> <p><code>/usr/bin/rsync</code></p>	
Hour of the Day to Start Local Database Backup	<p>Time of day that you want the GUI server to backup the database. Type a 2 digit number representing the time of day in a 24 hour clock notation (00 through 23). For example, if you want the backup to begin at 4:00 AM, type 04; if at 4:00 PM, type 16. We recommend that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI server completes the daily backup process within the hour specified every day.</p> <p>By default, the GUI server performs the daily backup within an hour after 2 AM.</p>	
Number of Local Database Backup Files Stored	<p>Total number of database backup files that the GUI server stores. When the GUI server reaches the maximum number of backup files you configure, it overwrites the oldest file.</p> <p>By default, the GUI server stores seven backup files.</p>	
Rsync Backup Timeout	Time value (in seconds) that the rsync utility waits before timing out backup operations. By default, the rsync utility waits 3600 seconds before timing out.	
Enable Logging	Enable logging related to local backup and HA.	
Device server Database Parameters	Parameters required for the Postgres Database used for the Device server. You must specify a port number, superuser name and password. By default, the Postgres Database uses port 5432; the superuser is "nsm".	

Table 10: Distributed Configuration—System Parameters (continued)

Parameter	Description	Your Value
Device Server ID	Unique ID assigned when you add the Device server.	
Password for GUI server Connection	Password assigned to the Device server enabling it to authenticate with the GUI server when attempting to connect.	

Prerequisites

Perform the prerequisite steps described as if you were installing the management system on the same server. See [“Prerequisite Steps” on page 19](#) for more information.

Installing the GUI Server

The NSM installer guides you through all the steps required to configure system parameters, and then NSM installer runs to completion.

To install the GUI server:

1. Navigate to the directory where you saved NSM installer file.
2. Run NSM installer.

On Linux, run the following command:

```
sh nsm2012.2_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2012.2_servers_sol_sparc.sh
```

The installation performs a series of pre installation checks to ensure that:

- The OS version and specified architecture are compatible.
- You are installing the correct software for your operating system.
- All of the needed software binaries and packages are present.

If any component is missing, NSM installer displays a message identifying the missing component:

```
Checking for platform-specific packages.....FAILED
The Following list of Packages are Required for NSM installation.
Please install the system update utility before continuing.
chkfontpath
```

- You have the correct version of the PostgreSQL database.
- You have correctly logged in as root and that the NSM user exists. The NSM installer creates the NSM user, if it does not already exist.

- For Linux servers, NSM installer checks whether iptables is running. If not, then NSM installer continues.

If iptables is running, the NSM installer displays a message similar to the following:

```
Checking for iptables service.....ok
Iptables is found to be running on the system. Please make sure the ports
7801 7802, 443, 7800, 7804 are open and available for NSM to run.

Please press enter to continue:
```

Ensure the required ports for NSM are available before continuing.

- The system has sufficient disk space and RAM.

The NSM installer stops any running servers.



NOTE: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that NSM installer successfully performed a task.
- “OK” indicates that the NSM installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the NSM installer performed a task or check, but it was unsuccessful. See the install log for information about the failure. This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of the install, the log might be in `/var/tmp`.

The NSM installer extracts the software payloads and prompts you to install NSM with the base license.

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh
```

```
##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers
```

```

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 2

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

```

3. The NSM installer prompts you to specify the components that you want to install. For example, enter **2** to specify that you want to install the GUI server only.



NOTE: If you have installed a previous version of the management system, then you might see different menu options.

```

Enter base directory location for management servers [/usr/netscreen]>

```

4. For a base license installation—that is, one that does not require the license key file—enter **y**. For an installation that requires a license key file, enter **n**. You can enter the license file path later. See [\[Unresolved xref\]](#) for information about obtaining license keys.
5. The NSM installer prompts you to specify a base directory in which to install the management server files.
6. Press Enter to accept the default **/usr/netscreen** directory, or type the full path name to a directory and then press Enter.

The NSM installer prompts whether you want to enable FIPS support.
7. If you require FIPS support, enter **y**. Otherwise, press Enter to accept the default value.

What happens next depends on whether you selected to install with a base license or with a license key file. If you are installing with a base license, skip step 8.
8. If you chose to install a license key file, the NSM installer displays the installation ID of the system prompts you to enter the license key file path.

```

The installation ID for this system is: 3FFFEA90278AA

```

Enter the License File Path>

- a. Use the installation ID to obtain a license key file from the LMS system and save it on your local drive as described in [\[Unresolved xref\]](#).
- b. Enter the license key file path.

The NSM installer validates the license key file.



NOTE: If the NSM installer prompts you for the license file and the license key is not available, press Ctrl+Z to exit the NSM installer.

The NSM installer prompts you to determine if you want this server to participate in an HA cluster.

9. Enter **n** if you do not want the server to participate in an HA cluster. If you are planning to configure NSM with HA enabled, enter **y**. Refer to "High Availability Overview" on page 47 for more information.

The NSM installer prompts you to configure the GUI server.

10. Configure the GUI server as follows:

- a. Type the directory location for storing the data files for the GUI server or press Enter to accept the default location `/var/netscreen/GuiSvr`.



NOTE: You cannot store files in an existing directory location. This feature safeguards against overwriting any existing data. If you specify an existing directory, the NSM installer prompts you to try again.

- b. Type the directory location for storing the database files for the GUI server or press Enter to accept the default location `/var/netscreen/GuiSvr/xdm/log`.



NOTE: You cannot store files in an existing directory location. This feature safeguards against overwriting any existing data. If you specify an existing directory, the NSM installer prompts you to try again.

The NSM installer prompts you to specify the management IP address of the GUI server.

- c. Type the IP address of the GUI server. This address should be the same as the server on which you are installing. The NSM installer sets the IP address and port number on the GUI server, enabling the Device server to start and connect. The Device server attempts to connect to the GUI server using port 7801 by default.
- d. Enter a port number for listening for messages from the NSM API. The default value is 8443. This parameter must be between 1025 and 65535.

The NSM installer prompts you to type a password for the superuser account. The initial administrator or superuser account is the account that you use when you first log in to NSM using the NSM user interface (UI). This account authenticates communication between the management system and the NSM UI. It possesses all administrative privileges by default.

- e. Type any text string longer than eight characters for the password. Type the password again for verification.



NOTE: Make a note of the password that you set for the superuser account. You need this when you first log in to the system.

- f. Enter a one-time password for the GUI server. This password authenticates this server to its peers in a high-availability configuration and to the central manager.

The NSM installer prompts you to determine if you want to use the Statistical Reports Server with the GUI server.

11. If you are not installing NetScreen-Statistical Report Server with NSM, enter **n**. If you are installing NetScreen-Statistical Report Server with NSM, enter **y**.

If you typed **y**, then the NSM installer prompts you to configure parameters required for the management system to work with the Statistical Report Server (that is, database type, database server IP address, database port, database name, database user name, database password). Refer to the *NetScreen-Statistical Report Server Installer's Guide* for more information about these parameters.

The NSM installer next creates a user in the NSM group for performing configuration file management actions and prompts for a password.

12. Enter a password for the configuration-file management (CFM) user.

Because the UNIX password cannot be saved in plain text format, the NSM installer prompts a second time to enter the same password to save in **guiSvr.cfg** file, which will be used for auto archival configuration settings.

The NSM installer next prompts if you want the server processes to be restarted automatically on failure.



NOTE: The CFM passwords for NSM and for UNIX must be identical, although NSM does not check that they are the same.

13. If you want the server processes to be restarted automatically in case of failure, enter **y**. If you do not want to restart server processes automatically, enter **n**.

The NSM installer next prompts you if you want the GUI server to perform a local backup of the database.

14. If you want to perform a daily backup of the database locally, enter **y**. If you do not want to back up the database locally, enter **n**.



NOTE: You must allow local backup if you want to specify remote backup.

If you specify that you want the NSM to perform backups, the NSM installer prompts you to configure options for the backup operation:

- a. Type a two-digit number (00 through 23) specifying the hour of day that you want the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, type **12**; for midnight, type **00**. Press Enter to accept the default setting of 02 (2:00 AM).
- b. Enter **n** so daily backups are not sent to a remote server. If you enter **y**, the NSM installer prompts you for an IP address for the remote backup server.



NOTE: If you want to perform backups to a remote server, make sure to establish a trust relationship with that server. See [“Establishing a Trust Relationship” on page 21](#)

- c. Type a number (from 0 to 7) to specify how many database backup files NSM stores. After NSM reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press Enter to accept the default setting of seven backup files.
- d. Type a number specifying how many seconds you want NSM to wait while performing backups until the process times out.
- e. Designate a directory location for locally storing the NSM database backup. Press Enter to accept the default location `/var/netscreen/dbbackup`.

The NSM installer prompts you to determine if you want to restart the GUI server after the installation process is completed.

15. To start the GUI server processes after the NSM installer has completed the installation process, enter **y**. The NSM installer will start the server processes with nsm user permissions.

If you do not want to start the server processes, enter **n**.



NOTE: When you restart your server, the GUI server and HA Server processes start automatically.

The NSM installer prompts you to verify your installation configuration settings.

16. Verify your settings. If the configuration settings are correct, enter **y** to proceed. If you enter **n**, the NSM installer returns to the previous prompt.

The installation proceeds automatically. The NSM installer performs the following actions:

- Installs the GUI server

- Installs the HA Server
- Performs post installation tasks such as removing the staging directory, and starting the GUI server

Several messages display to confirm the installation progress. The NSM installer runs for several minutes, and then exits.



NOTE: If you are installing NSM for the first time on a Solaris server, you must reboot the server after installation.

The installer generates a log file with the output of the installation commands for troubleshooting purposes.

The naming convention used for the installation log file is: **netmgtInstallLog.current date current time**.

For example, if you ran the NSM installer on December 1, 2003 at 6:00 PM, the installation log file would be named **netmgtInstallLog.20031201180000**.



NOTE: After the installation finishes, it indicates the name of the installation log file and the directory location where it is saved.

Typical Output for Installing a GUI Server in a Distributed Configuration

The following example shows installation of a GUI server in a distributed configuration:

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok
```

```
##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 2

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]>

##### GUI SERVER SETUP DETAILS #####

The GUI Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/GuiSvr. Because
the user data (including database data and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/GuiSvr]>

The GUI Server stores all of the database logs under a single directory.
By default, this directory is /var/netscreen/GuiSvr/xdm/log. Because
the database log can grow to be quite
large, it is sometimes desirable to place this log in another
partition.
Please enter an alternative location for this log if
so desired, or press ENTER for the location specified in the
brackets.
Enter database log directory location [/var/netscreen/GuiSvr/xdm/log]>

Enter the management IP address of this server [10.157.48.108]>

Enter the https port for NBI service [8443]>

Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter the one-time password for this Gui Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

CFM password for user 'cfmuser'
Enter password (password will not display as you type)>
```

```

Please enter again for verification
Enter password (password will not display as you type)>
Enter the same password again for CFM user
Changing password for user cfmuser.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Will server processes need to be restarted automatically in case of a failure?
(y/n) [y]>

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

Enter database backup directory [/var/netscreen/dbbackup]>

##### POST-INSTALLATION OPTIONS #####

Start server(s) when finished? (y/n) []> y

##### CONFIRMATION #####

About to proceed with the following actions:
- Install GUI Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine will have base license with maximum 25 devices
- This machine does not participate in an HA cluster
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdb/log
- Use IP address 10.157.48.108 for management
- Use port 8443 for NBI Service
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- Servers will be restarted automatically in case of a failure
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Start server(s) when finished: Yes

Are the above actions correct? (y/n)> y

##### PERFORMING INSTALLATION TASKS #####

```

```

----- INSTALLING GUI Server -----
Looking for existing RPM package.....ok
Removing existing GUI Server RPM.....ok
Installing GUI Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in GUI Server config file(s).....ok
Setting permissions for GUI Server.....ok
Running generateMPK utility.....ok
Running fingerprintMPK utility.....ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Enabling GUI Server start script.....ok
Enabling HA Server start script.....ok

##### PERFORMING POST-INSTALLATION TASKS #####
Converting GuiSvr SetDB to XDB .....ok
Loading GuiSvr XDB data from init files .....ok
ok
Running webproxy Cert Generation.....ok
Removing staging directory.....ok
Starting GUI Server.....ok
Starting HA Server.....ok

NOTES:
- Installation log is stored in
/usr/netscreen/GuiSvr/var/errorLog/netmgtInstallLog.20080902141953

- This is the GUI Server fingerprint:
E3:B6:5F:30:BE:6A:35:37:BD:9B:04:AB:95:BA:36:F3:86:D0:B4:2F
You will need this for verification purposes when logging into the GUI
Server. Please make a note of it.

[root@C73-16 ~]#

```

Installing the User Interface

Install the User Interface. See [“Installing the User Interface”](#) on page 39 for more information on installing the User Interface (UI).

Adding the Device Server in the User Interface

After you have installed the UI, you need to add the Device server and configure the following:

- Device Server ID
- Password for GUI Server Connection

This information enables the Device server to establish a connection with the GUI server.

To add the Device server:

1. From the UI **Administrate** panel, select **Server Manager > Server**.
 2. In the **Device Server** area, click the **+** icon. The Device Server dialog box appears.
 3. In the **Name** box, enter the name of the Device Server.
 4. In the **IP Address** box, enter the IP address of the Device Server.
 5. In the **Password for GUI Server Connection** box, enter the DevSvr one-time password you specified when installing the GUI server.
 6. If you are using a Mapped IP address (MIP), use the **General** tab, and click the **Add** icon (+) in the MIP section. The New MIP dialog box appears. Enter the mapped IP address and port of the Device Server in the fields provided.
- NSM sets the Device Server Manager port to 7800 by default. It also assigns an ID to the Device Server automatically (this ID appears in the Device Server ID box).
7. The default Device Server Manager port is set by NSM to 7800. You can edit this value.
 8. (Optional) If you wish to configure polling attributes, use the Device Polling tab. Device polling attributes enable you to configure the intervals with which the Device Server retrieves statistics from the managed devices in your network. These statistics appear in the Device Monitor and Realtime Monitor.
 9. Click **OK** to save your settings.



NOTE: Make a note of the Device Server ID and the Password for GUI Server Connection. You will need this when you install the Device Server.

Installing the Device Server

The NSM installer guides you through all the steps required to configure the system parameters and then the NSM installer runs to completion.



NOTE: Before installing the Device Server, verify that the GUI server is running. After you install the Device Server, the NSM installer starts the Device Server by default. If the GUI server is not already running, the Device Server will fail to connect to it.

To install NSM on the Device Server:

1. Navigate to the directory where you have saved the NSM installer file.
2. Run the NSM installer.

On Linux, run the following command:

```
sh nsm2012.2_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2012.2_servers_sol_sparc.sh
```

The installation begins automatically by performing a series of preinstallation checks.

The NSM installer extracts the software payloads and prompts you to specify the components of NSM that you want to install.

3. Enter **1** to specify that you want to install the Device Server only.



NOTE: If you installed a previous version of NSM, then you may have different menu options.

The NSM installer prompts you to install NSM with the base license.

4. Enter **y** or **n**. The NSM installer prompts you to specify a base directory in which to install the management server files.
5. Press Enter to accept the default **/usr/netscreen** directory, or type the full path to a directory and press Enter.

The NSM installer prompts whether you want to enable FIPS support.

6. If you require FIPS support, enter **y**. Otherwise, press Enter to accept the default value.

The NSM installer prompts you to specify if you want the server to be part of an HA cluster.

7. If you do not want the server to participate in an HA cluster, enter **n**. If you are planning to configure NSM with HA enabled, enter **y**. Refer to "High Availability Overview" on page 47 for more information.

The NSM installer prompts you to configure the Device Server.

8. Configure the Device Server as follows:

- a. Type the directory location for storing the Device Server data files or press Enter to accept the default location `/var/netscreen/DevSvr`.

The NSM installer prompts you to enter parameters assigned by the UI to this Device Server.

- b. Type the Device Server ID.

The NSM installer prompts you to type the one-time password for this Device Server.

- c. Type the one-time password for the GUI server connection. The one-time password must be a minimum of eight characters.

The NSM installer prompts you for the IP address and port number of the running GUI server. This address is required to enable the Device Server to communicate with the GUI server.

- d. Type the IP address of the running GUI server.

The NSM installer sets the IP address enabling the Device Server to connect. It attempts to connect to the GUI server using port 7801 by default.

The NSM installer prompts you to determine if you want to restart the server processes automatically in case of a failure.

9. If you want the server processes to be restarted automatically in case of failure, enter **y**. If you do not want to restart the server processes, enter **n**.

The NSM installer next prompts you to determine if you want to perform a daily backup of the database locally. If you installed and configured the local database backup on the GUI server, then you are required to install and configure the option on the Device Server.

10. If you want the Device Server to perform a backup of the database locally, enter **y**. If you do not want the Device Server to perform a backup, enter **n**.



NOTE: You must allow local backup if you want to specify remote backup.

If you specified that you want the Device Server to perform automatic backups, the NSM installer prompts you to configure options for the backup operation:

- a. Type a two-digit number (00 through 23) to specify the hour of day that you want NSM to perform the daily backup operation. For example, if you want NSM to perform the daily backup operation at noon, type **12**; for midnight, type **00**. Press Enter to accept the default setting of 02 (2:00 AM).
- b. Enter **n** so daily backups are not sent to a remote server. If you enter **y**, the NSM installer prompts you to enter the IP address of the remote backup server.
- c. Type a number (from 0 to 7) to specify how many database backup files to store. After NSM reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press Enter to accept the default setting of seven backup files.

- d. Type a number specifying how many seconds you want the management system to wait while performing backups until the process times out.
- e. Designate a directory location for locally storing the NSM database backup. To accept the default location, `/var/netscreen/dbbackup`, press Enter.

The NSM installer prompts you to configure the Device Server database.

11. Configure the Device Server database as follows:
 - a. Enter a port number for the Device Server database.
 - b. Enter a name for the database super user. If you specify a user that does not already exist, the NSM installer prompts you to enter a password for the database super user. Enter the password again for verification.

The NSM installer prompts you to determine if you want to restart the Device Server after the installation process is completed.

12. To start the Device Server after the NSM installer has completed the installation process, enter **y**. The NSM installer will start the process with nsm user permissions. If you do not want the Device Server to start automatically, enter **n**.



NOTE: When you reboot your server, the Device Server starts automatically.

The NSM installer prompts you to verify your installation configuration settings.

13. Verify your settings. If the configuration settings are correct, enter **y** to proceed. If you enter **n**, the NSM installer returns to the previous prompt.

If you confirmed your settings, the installation proceeds automatically. The NSM installer proceeds to perform the following actions:

- Installs the Device Server.
- Installs the HA Server.
- Performs post installation tasks.



NOTE: If you are installing NSM for the first time on a Solaris server, you must reboot the server after installation.

Typical Output for Installing a Device Server in a Distributed Configuration

The following example shows installation of a Device Server in a distributed configuration.

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
```

```

Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 1

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]>

##### DEVICE SERVER SETUP DETAILS #####

The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

Enter the ID assigned by the GUI to this Device Server (1-65535) []> 1

Enter the one-time password for this Device Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

To enable the Device Server to communicate with the GUI Server, you must
provide the IP address of the running GUI Server
Enter the IP address of the running GUI Server []> 10.157.48.108
##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

```

```
Will server processes need to be restarted automatically in case of a failure?
(y/n) [y]>

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

Enter database backup directory [/var/netscreen/dbbackup]>

##### DEVSVR DB SETUP DETAILS #####

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

##### POST-INSTALLATION OPTIONS #####

NOTE: Do not start up the Device Server unless you have already added it to
the system from the UI.
Start server(s) when finished? (y/n) []> n

##### CONFIRMATION #####

About to proceed with the following actions:
- Install Device Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine does not participate in an HA cluster
- Store Device Server data in /var/netscreen/DevSvr
- Connect to GUI Server at 10.157.48.108:7801
- Servers will be restarted automatically in case of a failure
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start server(s) when finished: No

Are the above actions correct? (y/n)> y

##### PERFORMING INSTALLATION TASKS #####
```

```

----- INSTALLING Device Server -----
Looking for existing RPM package.....ok
Removing existing Device Server RPM.....ok
Installing Device Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in Device Server config file(s).....ok
Setting permissions for Device Server.....ok
----- Setting up PostgreSQL for DevSvr -----
Setting up PostgreSQL for DevSvr.....ok
Installation of Device Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Enabling Device Server start script.....ok
Enabling HA Server start script.....ok

##### PERFORMING POST-INSTALLATION TASKS #####
Running nacnCertGeneration.....ok
Running idpCertGeneration.....ok
Removing staging directory.....ok

NOTES:
- Installation log is stored in
  /usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20080902144922

[root@C73-16 ~]#

```

Installing NSM with an IPv6 Management Address

Beginning in NSM2012.2R10, NSM can be installed with an IPv6 management address for a distributed installation.



NOTE: You must configure the IPv6 address in the NSM server before starting the installation.

An example of the output for a typical distributed NSM installation is as follows:

- [Primary GUI Server Output on page 70](#)
- [Primary Dev Server Output on page 74](#)

Primary GUI Server Output

```
[root@nsm-b3-vm7 ~]# sh nsm2012.2R10_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
WARNING:
Please make sure the following lines are present in the /etc/sysctl.conf file.
kernel.shmmax= 402653184
The install will exit if they aren't present. Please Reboot the system before
continuing
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if selinux is enabled.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 2

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

Select Device Schema to be loaded in NSM

1) Load all Device Family Schemas
2) Load Screen OS Device Schema only (Screen OS)
3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
Enter selection (1-3)[1]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y
```

```

Is this machine the primary server for the HA cluster? (y/n) [y]>
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### GUI SERVER SETUP DETAILS #####

Will the GUI Server data directory be located on a shared disk partition? (y/n)
[n]>

The GUI Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/GuiSvr. Because
the user data (including database data and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/GuiSvr]>

The GUI Server stores all of the database logs under a single directory.
By default, this directory is /var/netscreen/GuiSvr/xdm/log. Because
the database log can grow to be quite
large, it is sometimes desirable to place this log in another
partition.
Please enter an alternative location for this log if
so desired, or press ENTER for the location specified in the
brackets.
Enter database log directory location [/var/netscreen/GuiSvr/xdm/log]>

Enter the type of management IP address of this server (4-IPv4 / 6-IPv6) [4]> 6
Enter the management IPv6 address of this server [fc00::10:205:1:95]>

Enter the https port for NBI service [8443]>

Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter the one-time password for this Gui Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

CFM password for user 'cfmuser'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>
Enter the same password again for CFM user
Changing password for user cfmuser.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

```

```
Enter the type of management IP address for primary HA server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the primary HA Server [fc00::10:205:1:95]>

Enter the type of management IP address for secondary server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the secondary HA Server []> fc00::10:205:1:97

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the type of machine's primary heartbeat link IP (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address for this machine's primary heartbeat link [fc00::10:205:1:95]>

Enter the type of machine's peer's primary heartbeat link IP (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the peer's primary heartbeat link [fc00::10:205:1:97]>

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter the type of IP address outside the HA cluster (4-IPv4 / 6-IPv6) [4]> 6
Enter an IP address outside of the cluster []> fc00::10:205:255:254

Enter the rsync replication timeout [3600]>

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the
secondary server, via ssh-keygen, is a requirement for the
```

```

remote replication to work properly.
Please reset the trust relationship with 'nsm' user.
Here are sample commands:
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]> y

Enter the type of IP address for remote backup machine (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address of the remote backup machine [fc00::10:205:1:97]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

##### POST-INSTALLATION OPTIONS #####

Start High Availability daemon processes when finished? (y/n) []> y

##### CONFIRMATION #####

About to proceed with the following actions:
- Install GUI Server
- Install High Availability Server
- This machine will have base license with maximum 25 devices
- Store base directory for management servers as /usr/netscreen
- All Device Families Schemas Load
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdb/log
- Use IP address fc00::10:205:1:95 for management
- Use port 8443 for NBI Service
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- IP address for the primary HA Server: fc00::10:205:1:95
- IP address for the secondary HA Server: fc00::10:205:1:97
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: fc00::10:205:1:95
- IP address for the peer's primary heartbeat link: fc00::10:205:1:97
- IP address for remote HA replications: fc00::10:205:1:97
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: fc00::10:205:255:254
- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600

```

- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: fc00::10:205:1:97
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Start High Availability daemon processes when finished: Yes

Are the above actions correct? (y/n)> y

Primary Dev Server Output

```
[root@nsm-b3-vm7 ~]# sh nsm2012.2R10_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
WARNING:
Please make sure the following lines are present in the /etc/sysctl.conf file.
kernel.shmmax= 402653184
The install will exit if they aren't present. Please Reboot the system before
continuing
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if selinux is enabled.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 1

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

Select Device Schema to be loaded in NSM
```

```

1) Load all Device Family Schemas
2) Load Screen OS Device Schema only (Screen OS)
3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
Enter selection (1-3)[1]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]>
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### DEVICE SERVER SETUP DETAILS #####

Will the Device Server data directory be located on a shared disk partition? (y/n)
[n]>

The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

Enter the ID assigned by the GUI to this Device Server (1-65535) []> 1

Enter the one-time password for this Device Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

To enable the Device Server to communicate with the GUI Server, you must
provide the IP address of the running GUI Server
Enter the type of IP address of the running GUI Server (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address of the running GUI Server []> fc00::10:205:1:97
##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the type of management IP address for primary HA server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the primary HA Server [10.205.1.95]> fc00::10:205:1:95

Enter the type of management IP address for secondary server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the secondary HA Server []> fc00::10:205:1:96

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

```

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
 The IP addresses entered here must be correct and match on both ends of the link for automatic failover to function correctly.

Enter the type of machine's primary heartbeat link IP (4-IPv4 / 6-IPv6) [4]> 6
 Enter the IP address for this machine's primary heartbeat link [fc00::10:205:1:95]>

Enter the type of machine's peer's primary heartbeat link IP (4-IPv4 / 6-IPv6) [4]> 6
 Enter the IP address for the peer's primary heartbeat link [fc00::10:205:1:96]>

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
 The heartbeat message interval times the number of missing heartbeats must equal at least this value.
 Using the defaults is recommended.
 Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs [4]>

An IP address outside the HA cluster is needed to monitor this server's network connection.
 Enter the type of IP address outside the HA cluster (4-IPv4 / 6-IPv6) [4]> 6
 Enter an IP address outside of the cluster []> fc00::10:205:255:254

Enter the rsync replication timeout [3600]>

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
 Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
 Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.
 Please reset the trust relationship with 'nsm' user.
 Here are sample commands:
 cd /home/nsm
 su nsm
 ssh-keygen -t rsa
 chmod 0700 .ssh
 -- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

BACKUP SETUP DETAILS

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm ...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]> y

```

Enter the type of IP address for remote backup machine (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address of the remote backup machine [fc00::10:205:1:96]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

##### DEVSVR DB SETUP DETAILS #####

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

##### POST-INSTALLATION OPTIONS #####

NOTE: Do not start up the Device Server unless you have already added it to
      the system from the UI.
Start High Availability daemon processes when finished? (y/n) []> n

##### CONFIRMATION #####

About to proceed with the following actions:
- Install Device Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- All Device Families Schemas Load
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store Device Server data in /var/netscreen/DevSvr
- Connect to GUI Server at fc00::10:205:1:97:7801
- Connect to GUI Server at fc00::10:205:1:97:7801
- IP address for the primary HA Server: fc00::10:205:1:95
- IP address for the secondary HA Server: fc00::10:205:1:96
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: fc00::10:205:1:95
- IP address for the peer's primary heartbeat link: fc00::10:205:1:96
- IP address for remote HA replications: fc00::10:205:1:96
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: fc00::10:205:255:254
- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: fc00::10:205:1:96
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm

```

- Postgres DevSvr Db password set for 'nsm'
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n)> y

Starting Server Processes Manually

If you did not specify the NSM installer to start the servers when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually, enter the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

The HA Server process automatically starts the GUI server and Device Server processes.

NSM server processes always run with NSM user permissions, even if you have root permissions when you start them.

Validating Management System Status

To validate the management system is started and running properly, we recommend that you view the status of all the running server processes (the HA server, Device Server, and GUI server) to confirm that all services are running. See [“Controlling the Management System” on page 251](#) for more information on manual commands that you can send to the HA Server, Device Server, and GUI server.

Next Steps

Now that you have completed installing the management system on separate servers, you are ready to begin managing your network. Refer to the *Network and Security Manager Administration Guide* for information describing how to plan and implement for your network. You can also refer to the *Network and Security Manager Online Help* for more task-specific information.

CHAPTER 4

Installing NSM with High Availability

This chapter describes how to install the Network and Security Manager (NSM) management system and configure it to provide for high availability. This installation includes performing any prerequisite steps, running the management system installer on a primary and secondary server, configuring both servers to failover in the event that the primary server is unavailable, running the User Interface installer, and validating that you have installed the management system successfully.

This chapter contains the following sections:

- [High Availability Overview on page 79](#)
- [Suggested Simple HA Installation Order on page 86](#)
- [Suggested Extended HA Installation Order on page 87](#)
- [Defining System Parameters on page 88](#)
- [Prerequisites on page 92](#)
- [Installing NSM 2012.2 on the Primary Server on page 95](#)
- [Installing NSM 2012.2 on the Secondary Server on page 109](#)
- [Example: Installing NSM in a Simple HA Configuration on page 109](#)
- [Installing the User Interface on page 121](#)
- [Configuring the HA Cluster in the UI on page 121](#)
- [Installing NSM In an Extended HA Configuration on page 124](#)
- [Next Steps on page 144](#)

High Availability Overview

NSM with high availability requires two physical servers:

- A primary server that runs on a server machine in active mode
- A secondary server that runs on a different server machine in standby mode

If for any reason the primary server becomes unavailable, then the secondary server takes over as the active management system.

HA Configuration Options

You have two main options for installing NSM in a high availability configuration:

- Install and configure the management system in an HA cluster on two server machines: the primary management system with the Device Server and GUI server on the same machine, and a secondary management system with the Device Server and GUI server together on another machine.
- Install and configure the management system in an HA cluster on four server machines: the primary management system with the Device Server and GUI server on separate machines and a secondary management system with the Device Server and GUI server on separate machines.

You can also install and configure HA clusters in either scenario with access to a shared disk.

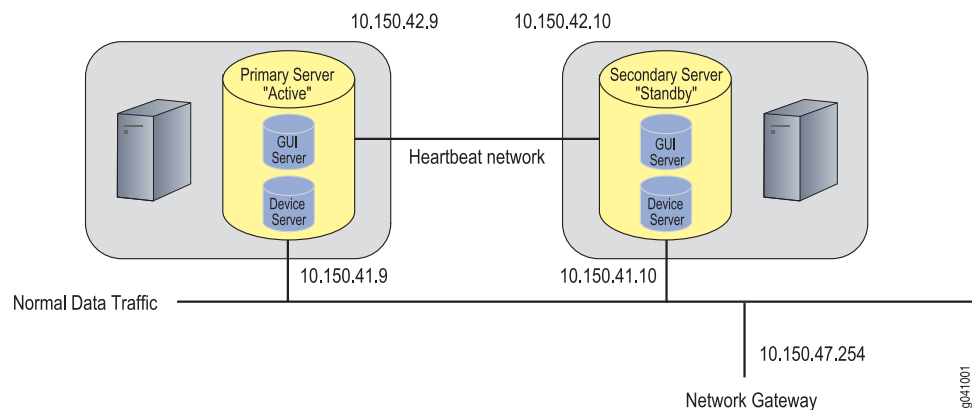
HA Requirements

Consider the following system requirements if you are planning on installing the management system for high availability:

- Both the primary and secondary management servers must share at least two network connections: there must be at least one network connection for data, and at least one network connection for heartbeat communication.
- The primary and secondary servers can be geographically separate.

Figure 6 on page 80 shows the physical setup of the primary and secondary management systems in a simple HA configuration.

Figure 6: Simple HA Management System Configuration



Communication Between Physical Servers

This section discusses the following aspects of communication between the physical servers:

- [Inter-server Communications on page 81](#)
- [HA Server on page 81](#)
- [Database Synchronization and Remote Replication on page 82](#)
- [HA Failover on page 82](#)
- [Restoring Connections on page 84](#)
- [Using a Shared Disk on page 84](#)
- [Creating a Trust Relationship Between Servers on page 85](#)
- [Server Authentication on page 85](#)

Inter-server Communications

Communications from your managed devices to the Device Server, from the Device Server to the GUI server, and from the GUI server to NSM UI clients are all TCP-based and make use of Juniper Networks' proprietary SSP (Secure Server Protocol). This ensures that both AES encryption and certificate-based authentication are used throughout. There are some exceptions:

- Certificate loading onto security devices running ScreenOS 5.0
- Initial setup of all managed devices to configure parameters on NSM using either Telnet or SSH

Managed ScreenOS devices always initiate the TCP session to the running Device Server on port 7800. The Device Server always initiates the TCP connection to the GUI server on port 7801. Device families that use the DMI interface use port 7804 to initiate communication. The UI client works slightly differently. It attempts connection to the primary GUI Server using TCP port 7801. Upon failure, the UI automatically attempts to connect to the secondary GUI server. This process is transparent to the Admin user. Note, however, that the IP address of the secondary GUI server now appears in the bottom left of the main UI window, and in the Server Monitor.

HA Server

Each physical server on which NSM runs contains a service called the HA Server (HaSvr). The HA Server:

- Controls and detects failures in both the GUI server and Device Server services, as well as the inter-server database synchronization and remote replication processes
- Starts and stops services

If you have installed the Device Server and GUI server on a single server, one HA Server controls all services.

Database Synchronization and Remote Replication

During normal HA operations, data is synchronized between the primary server and secondary server. The HA Server controls this synchronization process. The HA Server makes use of `rsync`, a utility supplied by the operating system, to transfer non-database files in each server's data directory (`/var/netscreen` by default). This process is known as remote replication.

The data in the configuration database is synchronized by using the high availability feature of DBXML. This process is known as database synchronization.

Objects such as PKI info and configuration data for the Device Server are synchronized. This action allows the secondary Device Server to have the information it needs to accept connections from managed devices and to create SSP connections to the GUI server. Without the synchronization process, the secondary Device Server would not have the same private key as the primary (in this case, if it attempts a connection to the GUI server, the SSP connection would be refused). This fact is important as it shows that a successful synchronization process must take place at least once after installation before the secondary Device Server can take over. A failover before the first synchronization (or before the first successful connection to the GUI server) could cause serious problems. After the installation process, you must check that this action has occurred.

Non-database files synchronization is performed automatically when the standby server comes up. Failover is disabled until first time synchronization finishes.

Some directories are excluded from the synchronization process. For example, the directory on the Device Server where log data is stored is excluded because of the potentially large size of your device log data. The complete list of directories that are excluded from the synchronization process are listed in a text file called:

```
/usr/netscreen/Hasvr/var/exclude.rsync
```



.....
NOTE: If you want the standby Device Server to access log data also on the active Device Server, you must connect both servers to an external shared disk.
.....



.....
NOTE: `Rsync` uses a temporary SSH connection to the peer server to perform the incremental backups. During synchronization, two SSH connections are open for the time it takes to complete the backup.
.....

HA Failover

During normal operations, both the primary and secondary management systems monitor the health of the other using a series of heartbeat communications. The HA Server sends heartbeat messages over the UDP 7802 channel between itself and its peer. It also pings an external device (normally the IP address of the network gateway) that you configure

during installation. This action is in addition to monitoring the services running on itself. Based on information the HA Server gathers about itself and its peer, it starts or stops all the services that reside on that machine.

Each server sends a heartbeat message to the other server every 15 seconds. If a series of consecutive heartbeat messages is not received by the primary server, the HA Server stops all services, and informs its peer of the problem. The peer HA Server then starts all its services. So for example, if you are running the primary GUI server and Device Server on Server1 and the secondary GUI server and Device Server on Server 2; and the primary GUI server fails—both the primary GUI server and primary Device Server on Server1 are shut down; and both the secondary GUI server and Device Server on Server 2 start up.



NOTE: For additional redundancy, we recommend that you install at least two additional heartbeat network connections. This installation protects against the heartbeat network connection from being the single point of failure for the entire system. For example, if a shared disk setup is used, in case one of the heartbeat network connections goes down, both servers would not consider the other server as dead, thus mounting the shared disk simultaneously, resulting in a corrupted file system. If you choose to install two network cards, we recommend that you use one dedicated interface for heartbeat communications, in addition to one for network communications.

In the event of a process failure on the primary server, the primary server proceeds as follows:

1. Shuts down all local server processes.
2. Synchronizes all information to disk.
3. Unmounts the shared partitions (if using a shared disk).
4. Signals to the secondary server that it is done shutting down.

The HA process in the primary server then enters an ERROR mode, and stays in that mode until you manually restart the HA Server.



NOTE: You cannot start or stop the Device Server and GUI server processes manually in an HA configuration. You must use the HA Server to control these services.



NOTE: To prevent the server from rebooting in a HA configuration that uses shared disks, you must ensure that none of the shared files are in use before stopping the HA Server process. If these files are in use (for example, by a vi or tail command), then the configured file system unmount command will fail, causing the server to reboot.

Restoring Connections

In the event that the GUI server fails over, the Device Server detects this status and automatically reconnects to the secondary GUI server.

If you are attempting to connect to the GUI server using the User Interface, you must enter the secondary server IP address to reconnect to the new GUI server IP address.



NOTE: After failover, it will take some time for the standby management system to become fully active with the replicated database. For large networks, this can take up to 10 minutes.

The Device Server receives SSP or SSH connections from each device it manages. All managed devices are configured with both primary and secondary Device Server IP addresses. During failover, the device connection with the primary Device Server will time out. The managed device will retry the connection, and then attempt connection to the secondary Device Server.

The Device Server also has a connection to the active GUI server. Like the managed devices in your network, the Device Server is configured with the primary and secondary IP address of the GUI server. Whenever a Device Server starts it will try to connect to the primary GUI server, then to the secondary, then back to the primary until it is successful.

Using a Shared Disk

On systems which contain a Device Server cluster, it is strongly recommended that you use a shared disk (although this is not a minimum requirement). This is an additional server, often optimized for data storage. Since the management system refers to this store simply as a path (specified during installation) the mechanism of communication to the store (for example, NFS relationship, SAN driver) and the type of media used is not relevant. It is also recommended that you create and test the shared disk prior to installation.

If an additional server is used as the shared data storage, a single point of failure is introduced. If you are using a shared disk setup, you need to ensure sufficient redundancy within the shared disk machine (for example, RAID, dual power supplies).



NOTE: In a Simple HA installation using a shared disk, ensure that the data directories of both the GUI server and the Device Server are on the same disk.



NOTE: If you are installing the management system for HA and you are using a shared disk, you must activate the primary server before activating the secondary server after the installation process.

Creating a Trust Relationship Between Servers

Rsync is run automatically by the HA Server and should not require any manual interaction. Under normal circumstances when connecting via SSH to a server, you are required to authenticate. The need for authentication is obviated by creating a trust relationship between the two servers. You do this by creating a public/private RSA key on each server and copying the public key to the peer. For more information, see [“Establishing an SSH Trust Relationship” on page 93](#).

Server Authentication

Communication between the Device Server and GUI server uses a proprietary TCP based protocol called SSP. This uses AES encryption and is similar to an IPSEC VPN tunnel. The authentication is achieved via certificates. Each side of the SSP tunnel has a private and public key. The public keys are exchanged during the first time the Device Server connects to the GUI server. This initial connection makes use of a OTP (one time password) which is configured on both Device Server and GUI server during installation.

Checking HA Status

Use the following script to get an accurate report on the state of the HA Server:

```
/usr/netscreen/HaSvr/utls/haStatus
```

An example of the output is provided below.

```
[root@NSM1 utls]# ./haStatus
=====
H/A process status
=====
Retrieving status...
highAvail (pid 1681).....ON
highAvailSvr (pids 2161).....ON
=====
State of the local and peer H/A server
=====
Local Server:
  192.168.0.152 running network-up      db-repl:in-sync
Peer Server:
  0.0.0.0      timed-out(error)        network-down    db-repl:n/a
```

You can view the same information by opening the following text file:

```
/usr/netscreen/HaSvr/var/HaStatus.txt
```

Viewing HA Error Logs

You can also view error logs generated by the HA Server by opening the following file:

```
/usr/netscreen/HaSvr/var/errorLog
```

If the HA Server is in error mode, the script appends log messages from the `/HaSvr/var/errorLog/highAvail.0` error log. You can use this script view error messages output for the server that the script is run in real time. If there is a problem preventing the status from being transmitted, observing the state from the UI only can be misleading.

HA Utilities

[Table 11 on page 86](#) lists and describes utilities that you can use to manage and maintain the HA server. All these utilities are located in `/usr/netscreen/HaSvr/utls`.

Table 11: HA Utilities

Parameter	Description
haStatus	Provides statistics on the HA processes.
replicateDB	Replicates data to the local or secondary server.
restoreDbFromBackup	Restores the local backup to current configuration.
validateBinaries	Checks if all binaries are present to run the server in HA.

Suggested Simple HA Installation Order

The following procedure summarizes the process for installing NSM in a simple HA configuration:

1. Define system parameters that you need to provide during the installation process.
2. Perform prerequisite steps.
3. Install NSM on the primary server.
4. Install NSM on the secondary server.
5. Install the User Interface. Log in to the primary management system and test that the primary management system is installed and working properly.
6. Allow the primary server to failover.
7. Reboot the UI and verify the connection to the secondary server.
8. Add your managed devices in the UI. Check the device connection to both Device Servers.

Suggested Extended HA Installation Order

The following procedure summarizes the process for installing NSM in an extended HA configuration. In general, we recommend that you install your primary servers first, test that they work properly, and then install the secondary servers. The order in which the four servers are installed is critical to the success. In an Extended HA configuration (for example, with four servers), the most important step is to ensure that the PKI information is shared correctly among the servers. A failure to do this step correctly could cause the Device Server- to GUI server connection to fail.

1. Define system parameters that you need to provide during the installation process.
2. Perform prerequisite steps.
3. Install the primary GUI server.
4. Install the primary Device Server.
5. Install the User Interface. Log in to the primary GUI server and test that the primary management system is installed and working properly.
6. Install the secondary Device Server.
7. Test that a successful remote replication occurs. You can do this by checking that files are located in the secondary server's `/var/netscreen/dbbackup` directory).
8. Allow the primary Device Server to failover. You can do this by stopping the primary DevSvr services or rebooting. This process may take several minutes because of the time taken to acknowledge failure, copy files from backup to active directories, then start the Device Server services. Use the `tail -f` command on the secondary server's HA Sever error log to view the progress.
9. Use the UI to test connectivity between secondary Device Server and the primary GUI server.

It is vital that the secondary Device Server remains the standby until after the first remote replication occurs. Failure to achieve this will result in the secondary Device Server using its own PKI information rather than that supplied by the primary Device Server. If this occurs, it will not have the correct private key to enable the SSP connection.
10. Install the secondary GUI server.

11. Test that a successful remote replication occurs. You can do this by checking that files are located in the secondary server's `/var/netscreen/dbbackup` directory. Again, it is important not to failover before a remote replication has successfully finished.
12. Allow the primary GUI server to failover.
13. Reboot the UI and verify the connection between the GUI server and Device Server.
14. Allow the primary Device Server to failover to test that it can connect to the secondary GUI server.
15. Add your managed devices in the UI. Check the device connection to both Device Servers.



NOTE: When configuring an extended HA installation, the GUI Servers are not replicated without a Device Server. Unless you add the Device Server before the secondary GUI server, the `shadow_server` entry is not created for the secondary GUI server.

Defining System Parameters

During the installation process, you are required to configure common system parameters such as the location of the directories where you want to store data for the GUI server and Device Server. We recommend that you define these system parameters before performing the management system installation.

Simple HA Configuration Parameters

Table 12 on page 88 describes the system parameters that you need to identify to install HA with the Device Server and GUI server on the same server machine.

Table 12: Simple HA Configuration—System Parameters

Parameter	Description	Your Value
Device Server data directory	<p>Directory location on the Device Server where device data is stored. Because the data on the Device Server can grow to be large, consider placing this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the Device Server stores data in:</p> <p><code>/var/netscreen/DevSvr/</code></p> <p>CAUTION: Do not place your data directory in <code>/usr/netscreen</code>. That path normally contains binary files and should not be used for data.</p>	

Table 12: Simple HA Configuration—System Parameters (continued)

Parameter	Description	Your Value
GUI Server data directory	<p>Directory location on the GUI server where user data is stored. Because the data on the GUI server can grow to be large, consider placing this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI server stores data in:</p> <p>/var/netscreen/GuiSvr/</p> <p>CAUTION: Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</p>	
GUI server database log directory	<p>Directory location on the GUI server where database logs are stored. Because the data on the GUI server can grow to be large, consider placing this log data in another partition. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI server stores data in:</p> <p>/var/netscreen/GuiSvr/xdb/log</p>	
Management IP address	<p>The IP address and port used by the running GUI server.</p> <p>The default is the IP address of the machine that you are installing on.</p>	
https port	<p>The port number for listening for messages from the NSM API. The range is from 1025 through 65535. The default value is 8443.</p>	
Initial “super” user password	<p>The password required to authenticate the initial user in the system. By default, the initial superuser account receives all administrative privileges in the system.</p>	
One-time GUI server password	<p>A password that authenticates the server to its peers in a high-availability configuration, or authenticates a regional server with a central manager.</p>	
Configuration file management password	<p>Configures a user and password for NSM to perform configuration file management operations, and a corresponding UNIX user and password. The NSM and UNIX passwords must be identical.</p>	
Primary HA Server IP address	<p>IP address of the primary server participating in the HA cluster.</p>	
Secondary HA Server IP address	<p>IP address of the secondary server participating in the HA cluster.</p>	

Table 12: Simple HA Configuration—System Parameters (continued)

Parameter	Description	Your Value
Heartbeat links between primary and secondary machine	<p>Number of heartbeat communication paths between the primary and secondary machine.</p> <p>By default, there is 1 communication link between the primary and secondary machine. This in addition to the data network link already existing in the primary/secondary HA Server IP address.</p>	
Shared password for heartbeat authentication.	This is the password that is required to authenticate heartbeat messages between the primary and secondary HA servers.	
IP Address for Primary machine's heartbeat link	IP address used for heartbeat communications on the primary server machine.	
Port used for heartbeat communication	<p>The port number used for heartbeat communications.</p> <p>The default port is 7802.</p>	
Heartbeat messages time interval	<p>Time interval (in seconds) between heartbeat messages.</p> <p>The default is 15 seconds.</p>	
Missing heartbeats before switchover occurs	<p>Number of missing heartbeat messages before automatic switchover to the secondary machine occurs.</p> <p>The default is 4 messages.</p>	
IP Address outside the HA cluster	Network IP address used to monitor this server's network connection.	
HA directory	<p>Directory location where high availability data is stored. Note that the same directory location is used if you configure this machine to perform local database backups.</p> <p>By default, the HA Server stores data at:</p> <p><code>/var/netscreen/dbbackup/</code></p>	
Path to the rsync utility executable	<p>Path to the rsync utility executable.</p> <p>The default path is:</p> <p><code>/usr/bin/rsync</code></p>	
Path to the ssh utility executable	<p>Path to the ssh utility executable.</p> <p>The default path is:</p> <p><code>/usr/bin/ssh</code></p>	

Table 12: Simple HA Configuration—System Parameters (continued)

Parameter	Description	Your Value
Remote Backup Machine IP Address	IP address of the machine where remote backups are sent. By default, the NSM installer sets this to the IP address of the secondary HA Server.	
Hour of the Day to Start Local Database Backup	Time of day that you want the GUI server to backup the database. Type a 2 digit number representing the time of day in a 24-hour day (00-23). For example, if you want the backup to begin at 4:00 AM, type 04 ; if at 4:00 PM, type 16 . We recommend that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI server completes the daily backup process within the hour specified every day. By default, the GUI server performs the daily backup within an hour after 2 AM.	
Number of Local Database Backup Files Stored	Total number of database backup files that the GUI server stores. When the GUI server reaches the maximum number of backup files you configure, it overwrites the oldest file. By default, the GUI server stores seven backup files.	
Rsync Backup Timeout	Time value (in seconds) that the rsync utility waits before timing out backup operations. By default, the rsync utility waits 3600 seconds before timing out.	
Enable Logging	Enable logging related to local backup and HA.	
Device Server Database Parameters	Parameters required for the Postgres Database used for the Device Server. You must specify a port number, superuser name and password. By default, the Postgres Database uses port 5432; the superuser is "nsm" .	

Extended HA Configuration Parameters

[Table 13 on page 91](#) describes additional system parameters that you need to identify to install HA with the Device Server and GUI server on separate server machines:

Table 13: Extended HA Configuration—System Parameters

Parameter	Description	Your Value
Device Server ID	Unique ID assigned when you add the Device Server.	
Password for GUI Server Connection	Password assigned to the Device Server enabling it to authenticate with the GUI server when attempting to connect.	

Shared Disk Parameters

If you are using a shared disk partition, the NSM installer prompts you to configure additional information. [Table 14 on page 92](#) identifies the additional system parameters that you need to identify to install HA with access to a shared disk.

Table 14: Shared Disk System Parameters

Parameter	Description	Your Value
Command to mount the shared disk partition	<p>The command to mount the shared data partition.</p> <p>The default command is:</p> <p>/bin/mount /var/netscreen/DevSvr</p>	
Command to unmount the shared disk partition	<p>The command to unmount the shared data partition. Before configuring this command, you must first verify that you have defined your mounts properly.</p> <p>The default command is:</p> <p>/bin/umount /var/netscreen/DevSvr</p>	
Command to check the integrity of the shared data partition	<p>The command to check the integrity on the shared data partition.</p> <p>The default command is:</p> <p>/sbin/fsck</p>	
Directory path for the shared disk	Directory path of the shared disk mount point.	

Prerequisites

Perform the steps described as if you were installing the management system using a standalone configuration. See [“Installing NSM in a Standalone Configuration” on page 15](#) for more information on installing the management system on the same server.

After you have performed the prerequisite steps in [“Prerequisite Steps” on page 19](#) we recommend that, before you install the management system with HA enabled, you perform the following additional steps as described in the following sections:

- [“Verifying That Shared Partitions Are Mounted Properly” on page 93](#)
- [“Verifying That All Required System Binaries Are Available” on page 93](#)
- [“Verifying That Clocks Are Synchronized” on page 93](#)
- [“Establishing an SSH Trust Relationship” on page 93](#)

Verifying That Shared Partitions Are Mounted Properly

If you are using a shared disk, verify that all partitions are mounted properly. You can verify this by checking the following files that each partition is listed on the appropriate mount point:

- **etc/fstab** (on Linux)
- **etc/vfstab** (on Solaris)

You also need to verify that all mounts are not set to restart automatically.

Verifying That All Required System Binaries Are Available

A shell archive script provided with your installation package verifies that all required system binaries are available.

To run the verification script:

1. Navigate to the HA Server utilities subdirectory (**/usr/netscreen/HaSvr/utls** by default).
2. Run the validation shell archive script. You can do so by running the following command:

```
./validateBinaries
```

Verifying That Clocks Are Synchronized

Before installing the management system with HA enabled, you must verify that the clocks on the server machines that you are using for the primary and secondary servers all have the same timestamp. This check is necessary because the failover logic determines whether to perform a restore from a database replicated remotely based on the timestamp of the last performed remote database replication.

Establishing an SSH Trust Relationship

You also need to ensure that you have established an SSH trust relationship between the primary and secondary servers.

The instructions for Linux are as follows:

1. Run the following commands on the primary server:

```
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
```



NOTE: If prompted to enter a pass phrase, leave the value blank.

The result of the process is the creation of a hidden directory called **.ssh** under **/home/nsm** which contains two text files (public and private key).

2. Run the following commands on the secondary server:

```
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
```



NOTE: If prompted to enter a passphrase, leave the value blank.

3. From the primary server, you then need to copy the public key called **.ssh/id_rsa.pub** to the secondary server manually and place it in **.ssh/authorized_keys**. For example, you would run the following command:

```
scp .ssh/id_rsa.pub root@<IP addr NSM2>:/root/.ssh/authorized_keys
```

4. From the secondary server, you then need to copy **.ssh/id_rsa.pub** to the **.ssh/authorized_keys** of the primary machine. For example:

```
scp .ssh/id_rsa.pub root@<IP addr NSM1>:/root/.ssh/authorized_keys
```



NOTE: If the remote machine already has established trust relationships with other computers, overwriting the **authorized_keys** file will break those trust relationships. Instead, copy the contents of the **id_rsa.pub** file onto a new line at the end of the **authorized_keys** file on the remote machine.

5. You should test connectivity via SSH from the primary server to the secondary server and vice versa. For example, to test SSH connectivity from NSM Server1 to NSM Server2, type the following command:

```
ssh root@<IP ADDRESS of Secondary Server>
```

6. Change the permissions of the **.ssh** directory on each machine to owner-only, using the following command:

```
chmod -r 0700 ~/.ssh
```

7. Validate that you do not receive a prompt to enter a password to access the secondary server.

If you do receive a password prompt, the remote database replication will not function properly. Check for errors in the steps for establishing a trust relationship and repeat the process from Step 1.

We recommend that you test the successful completion of this part of the installation process by opening an SSH connection to the peer server.

Installing NSM 2012.2 on the Primary Server

After you have successfully performed all prerequisite steps, you can install NSM 2012.2 on your primary server.

To install the primary server with high availability (HA) configured:

1. Load the NSM installer software onto the server where you want to use NSM. You can download the NSM installer from the [Juniper Networks Web site](#).
2. Navigate to the directory where you saved the NSM installer file. We recommend that you save the NSM installer in the `/var/tmp` subdirectory.
3. Run the management system installer.

On Linux, run the following command:

```
sh nsm2012.2_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2012.2_servers_sol_sparc.sh
```

The installation begins automatically by performing a series of pre installation checks. The NSM installer ensures that:

- The OS version and specified architecture are compatible.
- You are installing the correct software for your operating system.
- All of the needed software binaries and packages are present.

If any component is missing, the NSM installer displays a message identifying the missing component:

```
Checking for platform-specific packages.....FAILED
The Following list of Packages are Required for NSM installation.
Please install the system update utility before continuing.
chkfontpath
```

- You have the correct version of the PostgreSQL database.
- You have correctly logged in as root and that the NSM user exists. The NSM installer creates the NSM user, if it does not already exist.
- For Linux servers, the NSM installer checks whether iptables is running. If not, then the NSM installer continues.

If iptables is running, the NSM installer displays a message similar to the following:

```
Checking for iptables service.....ok
Iptables is found to be running on the system. Please make sure the ports
7801 7802, 443, 7800, 7804 are open and available for NSM to run.

Please press enter to continue:
```

Ensure the required ports for NSM are available before continuing.

- The system has sufficient disk space and RAM.

The NSM installer stops any running servers.



NOTE: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the NSM installer successfully performed a task.
- “OK” indicates that the NSM installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the NSM installer performed a task or check, but it was unsuccessful. See the install log for information about the failure. This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of the install, the log might be in `/var/tmp`.

The NSM installer extracts the software payloads and prompts you to install NSM with the base license.

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 3
```

```
Enter base directory location for management servers [/usr/netscreen]>
```

4. The NSM installer prompts you to specify the components of NSM that you want to install. Type **3** to specify that you want to install both the GUI server and the Device Server.



NOTE: If you have installed a previous version of the management system, then you might see different menu options.

The NSM installer prompts you to specify a base directory in which to install the management server files.

```
Do you want to do NSM installation with base license? (y/n) [y]>
```

5. For a base license installation—that is, one that does not require the license key file—enter **y**.

For an installation that requires a license key file, enter **n**. You will enter the license file path later. See “[Introduction](#)” on [page 3](#) for information about obtaining license keys.

6. To accept the default **/usr/netscreen** directory, press Enter, or enter the full path name to a directory.

The NSM installer prompts whether you want to enable FIPS support.

7. If you require FIPS support, enter **y**. Otherwise, press Enter to accept the default value.

What happens next depends on whether you selected to install with a base license or with a license key file. If you are installing with a base license, skip [Step 8](#).

8. If you chose to install a license key file, the NSM installer displays the installation ID of the system prompts you to enter the license key file path.

```
The installation ID for this system is: 3FFFEA90278AA
```

```
Enter the License File Path>
```

- a. Use the installation ID to obtain a license key file from the LMS system and save it on your local drive as described in [\[Unresolved xref\]](#).
- b. Enter the license key file path.

The NSM installer validates the license key file.



NOTE: If the NSM installer prompts you for the license file and the license key is not available, press **Ctrl+Z** to exit the NSM installer.

The NSM installer prompts you to determine if you want this server to participate in an HA cluster.

9. For the server to participate in an HA cluster, enter **y**.

The NSM installer prompts you to specify if the current server will act as the primary server for the HA cluster.

10. To specify the current server as the primary server for the HA cluster, enter **y**.

The NSM installer prompts you for information about the Device Server.

11. Configure the Device Server as follows:

- a. If you are not using a shared disk, enter **n**. If the Device Server data directory is located on a shared disk partition, enter **y**. If you are using a shared disk partition, the NSM installer prompts you to enter additional parameters required to mount and unmount the partition. Refer to [“Shared Disk Parameters” on page 92](#) for more information.
- b. Type the directory location for storing the Device Server data files or press Enter to accept the default location **/var/netscreen/DevSvr**.



NOTE: You cannot store files in an existing directory location. This feature safeguards against overwriting any existing data. If you specify an existing directory, the NSM installer prompts you to try again.

The NSM installer prompts you to specify information about the GUI server data files.

12. Configure the GUI server as follows:

- a. If you are not using a shared disk, enter **n**. If the GUI server data directory is located on a shared disk partition, enter **y**. If you are using a shared disk partition, the NSM installer prompts you to enter additional parameters required to mount and unmount the partition. Refer to [“Shared Disk Parameters” on page 92](#) for more information.
- b. Type the directory location for storing the GUI server data files or press Enter to accept the default location **/var/netscreen/GuiSvr**.
- c. Type the directory location for storing the GUI server database log files or press Enter to accept the default location **/var/netscreen/GuiSvr/xdb/log**.

The NSM installer prompts you to specify the management IP address for the server.

- d. Type the management IP address for the server. This address should be the same IP address as the server that you are installing on. The NSM installer sets the IP address and port number on the GUI server enabling the Device Server to connect. The Device Server attempts to connect to the GUI server using port 7801 by default.
- e. Enter a port number for listening for messages from the NSM API. The default value is 8443. This parameter must be between 1025 and 65535.

The NSM installer prompts you to type a password for the superuser account. The initial administrator or superuser account is the account that you use when you first log in to NSM using the NSM user interface (UI). This account authenticates communication between the management system and the NSM UI. It possesses all administrative privileges by default.

- f. Type any text string longer than eight characters for the password. Type the password again for verification.



NOTE: Make a note of the password that you set for the superuser account. You need this when you first log in to the UI.

- g. Enter a one-time password for the GUI server. This password authenticates this server to its peers in a high-availability configuration and to a central manager.

The NSM installer prompts you if you want to use a Statistical Report Server with the GUI server.

13. If you are not installing NetScreen-Statistical Report Server with NSM, enter **n**. If you are installing NetScreen-Statistical Report Server with NSM, enter **y**.

If you entered **y**, the NSM installer prompts you to configure parameters required for the management system to work with the Statistical Report Server (that is, database type, database server IP address, database port, database name, database username, database password). Refer to the *NetScreen-Statistical Report Server Installer's Guide* for more information about these parameters.

The NSM installer next creates a user in the NSM group for performing configuration file management actions and prompts for a password.

14. Enter a password for the configuration-file management (CFM) user.

Because the UNIX password cannot be saved in plain text format, the NSM installer prompts a second time to enter the same password to save in **guiSvr.cfg** file, which will be used for auto archival configuration settings.

The NSM installer next prompts if you want the server processes to be restarted automatically on failure.



NOTE: The CFM passwords for NSM and for UNIX must be identical, although NSM does not check that they are the same.

15. Configure the HA cluster as follows:

- a. Type the IP address for the primary HA Server.
- b. Type the IP address for the secondary HA Server.
- c. Type a shared password that will be used for authentication of the heartbeat links between the primary and secondary servers.



NOTE: Make a note of the shared password that you set for the heartbeat authentication. You need to configure the same password when installing NSM on the secondary server.

- d. Type the number of heartbeat links between the primary and secondary machines.
- e. Type the IP address for this machine's primary heartbeat link.
- f. Type the IP address for the peer's primary heartbeat link.
- g. Type the port number used for heartbeat communication.
- h. Enter a time interval in seconds between heartbeat messages.



NOTE: For larger deployments (that is, more than 1000 managed devices), increase the default heartbeat interval to a value proportional to the number of devices that you are managing greater than 1000 devices. For example, the default heartbeat interval is 15 seconds. This interval is appropriate for deployments of fewer than 1000 managed devices. If you plan to use NSM to manage more than 1000 devices, we recommend that you set the heartbeat interval to 30 seconds. As a general rule, we recommend that you double the timeout interval for every 1000 devices that you are managing.

- i. Enter the number of missing heartbeat messages before automatic switchover occurs.
- j. Enter an IP Address outside the cluster to be used to monitor this server's network connection.
- k. Type a number specifying how many seconds you want the management system to wait while performing backups until the process times out.
- l. Designate a directory location for locally storing the NSM database with HA backup. Press Enter to accept the default location `/var/netscreen/dbbackup`.
- m. Type the full path where the rsync utility is located.
- n. Enter the full path to the ssh executable.



NOTE: If you are installing NSM on Solaris, the path to the SSH executable is typically different than the default setting of `/usr/bin/rsync`. It is typically `/usr/local/bin`.

- 16. The NSM installer prompts you to ensure that a trust relationship is established between the primary and secondary servers. If you have already established the trust relationship, press Enter to continue with the installation. If you have not yet established a trust relationship, press Ctrl + Z to abort the installation, establish a trust relationship as described in ["Establishing an SSH Trust Relationship" on page 93](#), and then restart the NSM installer.

The NSM installer next prompts you to determine if you want to perform daily backups of the database locally.

17. If you want NSM to perform a local backup of the database on a daily basis, enter **y**.

If you do not want to back up the database locally, enter **n**.



NOTE: You must allow local backup if you want to specify remote backup.

If you specify that you want to perform automatic backups, the NSM installer prompts you to configure options for the backup operation:

- a. Type a two-digit number (00 through 23) specifying the hour of day that you want NSM to perform the daily backup operation. For example, if you want NSM to perform the daily backup operation at noon, type **12**; for midnight, type **00**. Press Enter to accept the default setting of 02 (2:00 AM).
- b. Enter **n** so daily backups are not sent to a remote server. If you enter **y**, the NSM installer prompts for an IP address for the remote backup server.



NOTE: If you want to perform backups to a remote server, make sure to establish a trust relationship with that server. See [“Establishing a Trust Relationship” on page 21](#)

- c. Type a number (from 0 to 7) to specify how many database backup files NSM stores. After the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press Enter to accept the default setting of seven backup files.
- d. Type a number specifying how many seconds you want NSM to wait while performing backups until the process times out.

The NSM installer prompts you to configure the Device Server database.

18. Configure the Device Server database as follows:

- a. Enter a port number for the Device Server database.
- b. Enter a name for the database superuser. If you specify a user that does not already exist, the NSM installer prompts you for a password. Enter the password again for verification.

The NSM installer prompts you to start the HA processes when installation is complete.

19. If you want to start the HA processes, enter **y**.

The NSM installer will start all processes with nsm user permissions.

20. Verify your settings. If the configuration settings are correct, enter **y** to proceed. If you enter **n**, the NSM installer returns to the previous prompt.

The NSM installer proceeds to perform the following actions:

- Installs the Device server.
- Installs the GUI server.
- Installs the HA server.
- Performs post installation tasks.

Several messages display to confirm the installation progress.

The NSM installer runs for several minutes, then returns you to the command prompt.



NOTE: If you are installing NSM for the first time on a Solaris server, you must reboot the server after installation.

Viewing the Management System Installation Log

The NSM installer generates a log file with the output of the installation commands for troubleshooting purposes.

The naming convention used for the installation log file is:

```
netmgtInstallLog.<current date><current time>
```

For example if you ran the NSM installer on December 1, 2003 at 6:00 PM, then the installation log file would be named:

```
netmgtInstallLog.20031201180000
```



NOTE: After the installation finishes, it indicates the name of the installation log file and the directory location where it is saved.

Installing NSM with an IPv6 Management Address

Beginning in NSM2012.2R10, NSM can be installed with an IPv6 management address for a high availability installation.



NOTE: You must configure the IPv6 address in the NSM server before starting the installation.

Typical Primary HA Server Output for a High Availability Installation

```
[root@nsm-b3-vm7 ~]# sh nsm2012.2R10_servers_linux_x86.sh
```

```

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
WARNING:
Please make sure the following lines are present in the /etc/sysctl.conf file.
kernel.shmmax= 402653184
The install will exit if they aren't present. Please Reboot the system before
continuing
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if selinux is enabled.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 3

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

Select Device Schema to be loaded in NSM

1) Load all Device Family Schemas
2) Load Screen OS Device Schema only (Screen OS)
3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
Enter selection (1-3)[1]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]>
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### DEVICE SERVER SETUP DETAILS #####

```

```
Will the Device Server data directory be located on a shared disk partition? (y/n)
[n]>
```

The Device Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/DevSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition.

Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

```
Enter data directory location [/var/netscreen/DevSvr]>
```

```
##### GUI SERVER SETUP DETAILS #####
```

```
Will the GUI Server data directory be located on a shared disk partition? (y/n)
[n]>
```

The GUI Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/GuiSvr. Because the user data (including database data and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition.

Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

```
Enter data directory location [/var/netscreen/GuiSvr]>
```

The GUI Server stores all of the database logs under a single directory. By default, this directory is /var/netscreen/GuiSvr/xdm/log. Because the database log can grow to be quite large, it is sometimes desirable to place this log in another partition.

Please enter an alternative location for this log if so desired, or press ENTER for the location specified in the brackets.

```
Enter database log directory location [/var/netscreen/GuiSvr/xdm/log]>
```

```
Enter the type of management IP address of this server (4-IPv4 / 6-IPv6) [4]> 6
Enter the management IPv6 address of this server [fc00::10:205:1:95]>
```

```
Enter the https port for NBI service [8443]>
```

```
Setting GUI Server address and port to fc00::10:205:1:95:7801 for Device Server
```

```
Please enter a password for the 'super' user
```

```
Enter password (password will not display as you type)>
```

```
Please enter again for verification
```

```
Enter password (password will not display as you type)>
```

```
Enter the one-time password for this Gui Server
```

```
Enter password (password will not display as you type)>
```

```
Please enter again for verification
```

```
Enter password (password will not display as you type)>
```

```
Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>
```

```
==> CFM user is set to 'cfmuser'
```

```

CFM password for user 'cfmuser'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>
Enter the same password again for CFM user
Changing password for user cfmuser.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the type of management IP address for primary HA server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the primary HA Server [fc00::10:205:1:95]>

Enter the type of management IP address for secondary server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the secondary HA Server []> fc00::10:205:1:97

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the type of machine's primary heartbeat link IP (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address for this machine's primary heartbeat link [fc00::10:205:1:95]>

Enter the type of machine's peer's primary heartbeat link IP (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the peer's primary heartbeat link [fc00::10:205:1:97]>

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter the type of IP address outside the HA cluster (4-IPv4 / 6-IPv6) [4]> 6
Enter an IP address outside of the cluster []> fc00::10:205:255:254

```

```

Enter the rsync replication timeout [3600]>

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the
secondary server, via ssh-keygen, is a requirement for the
remote replication to work properly.
Please reset the trust relationship with 'nsm' user.
Here are sample commands:
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]> y

Enter the type of IP address for remote backup machine (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address of the remote backup machine [fc00::10:205:1:97]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

##### DEVSVR DB SETUP DETAILS #####

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

##### POST-INSTALLATION OPTIONS #####

Start High Availability daemon processes when finished? (y/n) []> y

##### CONFIRMATION #####

About to proceed with the following actions:
- Install Device Server
- Install GUI Server
- Install High Availability Server
- This machine will have base license with maximum 25 devices

```

```

- Store base directory for management servers as /usr/netscreen
- All Device Families Schemas Load
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdm/log
- Use IP address fc00::10:205:1:95 for management
- Use port 8443 for NBI Service
- Connect to GUI Server at fc00::10:205:1:95:7801
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- IP address for the primary HA Server: fc00::10:205:1:95
- IP address for the secondary HA Server: fc00::10:205:1:97
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: fc00::10:205:1:95
- IP address for the peer's primary heartbeat link: fc00::10:205:1:97
- IP address for remote HA replications: fc00::10:205:1:97
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: fc00::10:205:255:254
- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: fc00::10:205:1:97
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start High Availability daemon processes when finished: Yes

```

```
Are the above actions correct? (y/n)> y
```

Starting Server Processes Manually

If you did not specify the NSM installer to start the servers when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually, enter the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

The HA Server process automatically starts the GUI server and Device Server processes.

NSM server processes always run with nsm user permissions, even if you have root user permissions when you start them.

Validating Management System Status

To validate the management system is started and running properly, we recommend that you view the status of all the running server processes (the HA, Device, and GUI Servers) to confirm that all services are running. For example:

```
/usr/netscreen/DevSvr/bin/devSvr.sh status
```

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh status
```

```
/usr/netscreen/HaSvr/bin/haSvr.sh status
```

If any service is not running, stop all three processes and restart them using the HA Server process.

If you are experiencing problems with the HA Server, run the following command for more detailed information:

```
/usr/netscreen/HaSvr/utls/haStatus
```

The haStatus utility provides additional information describing the state and status of the local/peer servers.

Other Useful Commands

[Table 15 on page 108](#) describes some useful commands which may assist in the installation and troubleshooting of your high availability configuration:

Table 15: Useful Installation and Troubleshooting Commands

Command	Description
less <filename>	Displays the contents of a text file. The up and down keys can be used to scroll. the letter q to quit.
netstat -n	Displays the current network connections without resolving any addresses
while sleep 1;do netstat -n grep 192.168.0.;done	Continually displays the command after the word "do." This command is useful if you are waiting for a server connection attempt of data sync.
clear	Clears the screen
vmstat 1	Gives a continuous output of system resource information. The figures at the end of the line give CPU statistics.

Installing NSM 2012.2 on the Secondary Server

After you have successfully installed the management system software on the primary server, run the management system installer on the secondary server. Follow the NSM installer prompts to configure the secondary server.



NOTE: If you are using a shared disk, you must stop the primary server before installing the secondary server. The secondary server and primary server must also run on the same operating system and share the same directory structure for all NSM software and data.



NOTE: If you are installing NSM for the first time on a Solaris server, you must reboot the server after installation.

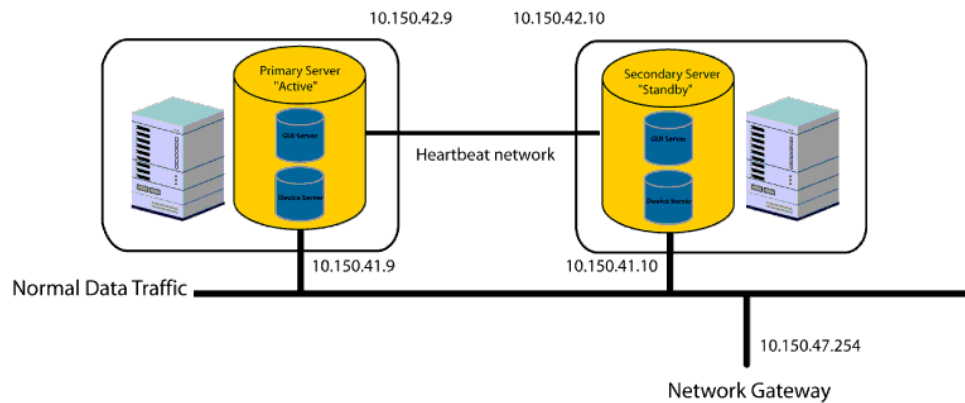
Example: Installing NSM in a Simple HA Configuration

The following example installs the management system in a simple HA configuration (GUI server and Device Server on the same server machine) with the following parameters:

- No shared disk
- No Statistical Report Server
- Only one heartbeat link between the primary/secondary servers
- IP Address of the primary HA server is 10.150.41.9
- IP Address of the secondary HA server is 10.150.41.10
- IP Address outside the HA Cluster is 10.150.47.254
- Daily local database backup
- Daily remote database backup
- Heartbeat link sent over remote replications/backups

Figure 7 on page 110 shows this configuration.

Figure 7: HA Configuration Example



Primary GUI Server and Device Server Installation

The following example shows the complete installer output for installing the primary GUI server and Device Server on the same server using the configuration described:

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 3

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>
```

```

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]>
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### DEVICE SERVER SETUP DETAILS #####

Will the Device Server data directory be located on a shared disk partition? (y/n)
[n]>

The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

##### GUI SERVER SETUP DETAILS #####

Will the GUI Server data directory be located on a shared disk partition? (y/n)
[n]>

The GUI Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/GuiSvr. Because
the user data (including database data and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/GuiSvr]>

The GUI Server stores all of the database logs under a single directory.
By default, this directory is /var/netscreen/GuiSvr/xdm/log. Because
the database log can grow to be quite
large, it is sometimes desirable to place this log in another
partition.
Please enter an alternative location for this log if
so desired, or press ENTER for the location specified in the
brackets.
Enter database log directory location [/var/netscreen/GuiSvr/xdm/log]>

Enter the management IP address of this server [10.150.41.9]>

Enter the https port for NBI service [8443]>

Setting GUI Server address and port to 10.150.41.9:7801 for Device Server

Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification

```

```
Enter password (password will not display as you type)>

Enter the one-time password for this Gui Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

CFM password for user 'cfmuser'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>
Enter the same password again for CFM user
Changing password for user cfmuser.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the IP address for the primary HA Server [10.150.41.9]>

Enter the IP address for the secondary HA Server []> 10.150.41.10

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.9]>
10.150.42.9

Enter the IP address for the peer's primary heartbeat link [10.150.41.10]>
10.150.42.10

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>
```

An IP address outside the HA cluster is needed to monitor this server's network connection.

Enter an IP address outside of the cluster []> 10.150.47.254

Enter the rsync replication timeout [3600]>

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.

Please reset the trust relationship with 'nsm' user.

Here are sample commands:

```
cd /home/nsm
```

```
su nsm
```

```
ssh-keygen -t rsa
```

```
chmod 0700 .ssh
```

```
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys
```

BACKUP SETUP DETAILS

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm ...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

DEVSVR DB SETUP DETAILS

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

POST-INSTALLATION OPTIONS

Start High Availability daemon processes when finished? (y/n) []> n

CONFIRMATION

About to proceed with the following actions:

- Install Device Server
- Install GUI Server
- Install High Availability Server

```

- Store base directory for management servers as /usr/netscreen
- This machine will have base license with maximum 25 devices
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdm/log
- Use IP address 10.150.41.9 for management
- Use port 8443 for NBI Service
- Connect to GUI Server at 10.150.41.19:7801
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- IP address for the primary HA Server: 10.150.41.9
- IP address for the secondary HA Server: 10.150.41.10
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.42.9
- IP address for the peer's primary heartbeat link: 10.150.42.10
- IP address for remote HA replications: 10.150.41.10
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start High Availability daemon processes when finished: No

```

Are the above actions correct? (y/n)> y

PERFORMING INSTALLATION TASKS

----- INSTALLING Device Server -----

```

Looking for existing RPM package.....ok
Removing existing Device Server RPM.....ok
Installing Device Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSR00T into start scripts.....ok
Filling in Device Server config file(s).....ok
Setting permissions for Device Server.....ok
----- Setting up PostgreSQL for DevSvr -----
Setting up PostgreSQL for DevSvr.....ok
Installation of Device Server complete.

```

----- INSTALLING GUI Server -----

```

Looking for existing RPM package.....ok

```

```

Removing existing GUI Server RPM.....ok
Installing GUI Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in GUI Server config file(s).....ok
Setting permissions for GUI Server.....ok
Running generateMPK utility.....ok
Running fingerprintMPK utility.....ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Disabling Device Server start script.....ok
Disabling GUI Server start script.....ok
Enabling HA Server start script.....ok

##### PERFORMING POST-INSTALLATION TASKS #####
Running nacnCertGeneration.....ok
Running idpCertGeneration.....ok
Converting GuiSvr SetDB to XDB .....ok
Loading GuiSvr XDB data from init files .....ok
ok
Running webproxy Cert Generation.....ok
Removing staging directory.....ok

NOTES:
- Installation log is stored in
/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20080902150909

- This is the GUI Server fingerprint:
  17:3E:1F:B9:69:29:3C:1F:ED:5D:53:7B:CE:AE:63:29:08:E2:DB:65
  You will need this for verification purposes when logging into the GUI
  Server. Please make a note of it.

[root@C73-16 ~]#

```

Secondary GUI Server and Device Server Installation Script

The following example shows the complete installer output for installing the secondary GUI server and Device Server on the same server using the configuration described:

```

[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok

```

```

Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 3

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]> n
WARNING: The servers need to be stopped on the primary server
during the installation of this software to avoid data corruption.

##### DEVICE SERVER SETUP DETAILS #####

Will the Device Server data directory be located on a shared disk partition? (y/n)
[n]>

The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

##### GUI SERVER SETUP DETAILS #####

Will the GUI Server data directory be located on a shared disk partition? (y/n)

```

```
[n]>
```

The GUI Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/GuiSvr. Because the user data (including database data and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition.

Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

```
Enter data directory location [/var/netscreen/GuiSvr]>
```

The GUI Server stores all of the database logs under a single directory. By default, this directory is /var/netscreen/GuiSvr/xdm/log. Because the database log can grow to be quite large, it is sometimes desirable to place this log in another partition.

Please enter an alternative location for this log if so desired, or press ENTER for the location specified in the brackets.

```
Enter database log directory location [/var/netscreen/GuiSvr/xdm/log]>
```

```
Enter the management IP address of this server [10.150.41.10]>
```

```
Enter the https port for NBI service [8443]>
```

```
Setting GUI Server address and port to 10.150.41.10:7801 for Device Server
```

Please enter a password for the 'super' user

```
Enter password (password will not display as you type)>
```

Please enter again for verification

```
Enter password (password will not display as you type)>
```

Enter the one-time password for this Gui Server

```
Enter password (password will not display as you type)>
```

Please enter again for verification

```
Enter password (password will not display as you type)>
```

```
Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>
```

```
==> CFM user is set to 'cfmuser'
```

CFM password for user 'cfmuser'

```
Enter password (password will not display as you type)>
```

Please enter again for verification

```
Enter password (password will not display as you type)>
```

Enter the same password again for CFM user

Changing password for user cfmuser.

New UNIX password:

BAD PASSWORD: it is based on a dictionary word

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

```
##### HIGH AVAILABILITY (HA) SETUP DETAILS #####
```

```
Enter the IP address for the primary HA Server []> 10.150.41.9
```

```
Enter the IP address for the secondary HA Server [10.150.41.10]>
```

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and

```

secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
The IP addresses entered here must be correct and match on both ends of
the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.10]>
10.150.42.10

Enter the IP address for the peer's primary heartbeat link [10.150.41.9]>
10.150.42.9

Enter the IP address that will be used for remote HA replications [10.150.41.9]>

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter an IP address outside of the cluster []> 10.150.47.254

Enter the rsync replication timeout [3600]>

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the
secondary server, via ssh-keygen, is a requirement for the
remote replication to work properly.
Please reset the trust relationship with 'nsm' user.
Here are sample commands:
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

##### BACKUP SETUP DETAILS #####

```

```

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

##### DEVSVR DB SETUP DETAILS #####

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

##### POST-INSTALLATION OPTIONS #####

Start High Availability daemon processes when finished? (y/n) []> n

##### CONFIRMATION #####

About to proceed with the following actions:
- Install Device Server
- Install GUI Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine will have base license with maximum 25 devices
- This machine participates in an HA cluster
- This server is the primary: No
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdm/log
- Use IP address 10.150.41.10 for management
- Use port 8443 for NBI Service
- Connect to GUI Server at 10.150.41.10:7801
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- IP address for the primary HA Server: 10.150.41.9
- IP address for the secondary HA Server: 10.150.41.10
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.42.10
- IP address for the peer's primary heartbeat link: 10.150.42.9
- IP address for remote HA replications: 10.150.41.9
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: n
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup

```

- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n)> y

PERFORMING INSTALLATION TASKS

----- INSTALLING Device Server -----

Looking for existing RPM package.....ok
Removing existing Device Server RPM.....ok
Installing Device Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in Device Server config file(s).....ok
Setting permissions for Device Server.....ok
----- Setting up PostgreSQL for DevSvr -----
Setting up PostgreSQL for DevSvr.....ok
Installation of Device Server complete.

----- INSTALLING GUI Server -----

Looking for existing RPM package.....ok
Removing existing GUI Server RPM.....ok
Installing GUI Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in GUI Server config file(s).....ok
Setting permissions for GUI Server.....ok
Running generateMPK utility.....ok
Running fingerprintMPK utility.....ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----

Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----

Disabling Device Server start script.....ok
Disabling GUI Server start script.....ok
Enabling HA Server start script.....ok

```

##### PERFORMING POST-INSTALLATION TASKS #####
Running nacnCertGeneration.....ok
Running idpCertGeneration.....ok
Running webproxy Cert Generation.....ok
Removing staging directory.....ok

NOTES:
- Installation log is stored in
/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20080902154907

- This is the GUI Server fingerprint:
F0:22:6D:62:D3:1C:0B:7E:F9:B7:58:84:BB:C4:2A:37:A2:AF:B2:13
You will need this for verification purposes when logging into the GUI
Server. Please make a note of it.

[root@C73-16 ~]#

```

Installing the User Interface

Install the NSM User Interface. See [“Installing the User Interface” on page 39](#). After you have installed the UI, launch the application and validate that you can connect to the primary server successfully.

Configuring the HA Cluster in the UI

After you have installed your primary and secondary servers, you must add information about your secondary servers in the UI and configure the HA Cluster. After you have done this, you must then update this configuration to all the managed devices in your network. In the event that the primary server fails, the managed devices will reattempt to connect to the management system using the Secondary Server IP Address.

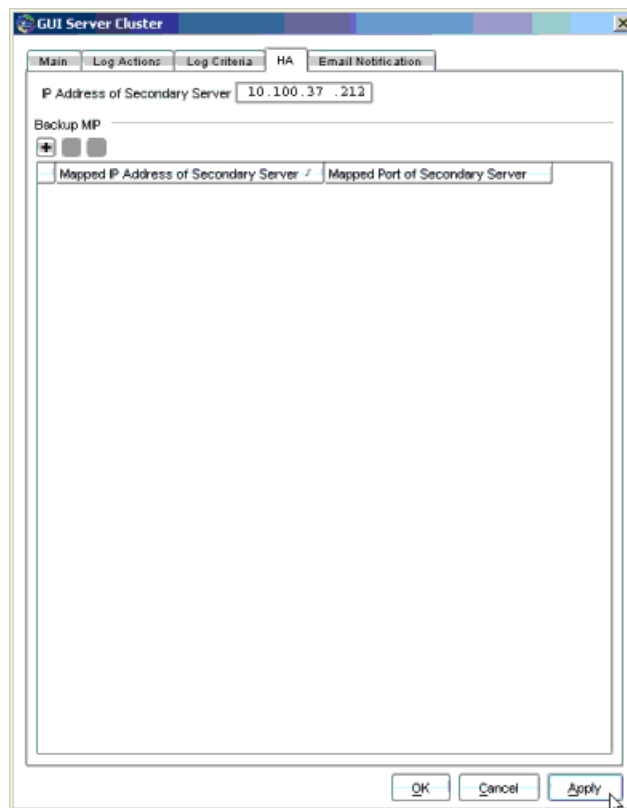
To add the secondary server:

1. From the NSM UI, select **Server Manager>Server**.
2. In the Device Server area, click the **+** icon. The Device Server dialog box appears.
3. In the Name box, enter the name of the Device Server.
4. In the IP Address box, enter the IP address of the Device Server.
5. In the Password for GUI server Connection box, enter the password you specified for the “super” user account, when you installed the GUI server.
6. If you are using a Mapped IP Address, use the General tab, and click in the MIP section. The New MIP dialog box appears. Enter the mapped IP address and port of the Device Server in the fields provided. You can also edit the Device Server Manager port and Device Server ID.
7. If you wish to configure polling attributes, use the Device Polling tab. Device polling attributes enable you to configure the intervals with which the Device Server retrieves statistics from the managed devices in your network. These statistics appear in the Device Monitor and Realtime Monitor. (Optional)
8. Click **OK** to save your settings.

To configure the GUI server Cluster:

1. From the NSM UI, select **Server Manager>Servers>GUI Server**, and then click on the **Edit** icon or right-click on the GUI server and select Edit to view all information available on the GUI server.
2. Use the Server Type list to select GUI server Cluster. The HA and Email Notification tabs become available.
3. Click to activate the HA tab. Configure the following parameters as shown in [Figure 8 on page 122](#):
 - a. Enter the IP Address of the Secondary Server.
 - b. Enter the Secondary GUI Server Manager Port (if applicable)
 - c. Mapped IP Address (if applicable)

Figure 8: Configuring the HA GUI Server Cluster



4. Click **Apply** when you are done.
5. (Optional) Click to activate the E-mail Notification tab. Configure the following parameters:
 - a. Enter the IP Address of the SMTP Server.
 - b. Enter the e-mail address referenced in the e-mail notification in the **From Email Address** field.

- c. Click the plus **+** button to add recipients of the e-mail notification. The New Add/Edit E-mail Address window appears enabling you to enter an e-mail address. Click **OK** when you are done.
 - d. Click the - button to remove recipients of the e-mail notification.
 - e. Click to select an e-mail address entry from the **To Email Address** list and click the **Edit** button to edit the e-mail address.
6. Click **Apply** when you are done.

To configure the Device Server Cluster:

1. From the NSM UI, select **Server Manager>Servers>Device Server**, then click on the **Edit** icon or right-click on the device server and select **Edit** to view all information available on the device server.
2. Use the **Server Type** list to select **Device Server Cluster**. The **HA** and **Email Notification** tabs become available.
3. Select the **HA** tab. Configure the following parameters as shown in [Figure 9 on page 123](#):
 - a. Enter the IP Address of the Secondary Server.
 - b. Enter the Secondary Device Server Manager Port (if applicable)
 - c. Enter the mapped IP Address and Port of the Secondary Server (if applicable)

Figure 9: Configuring the HA Device Server Cluster

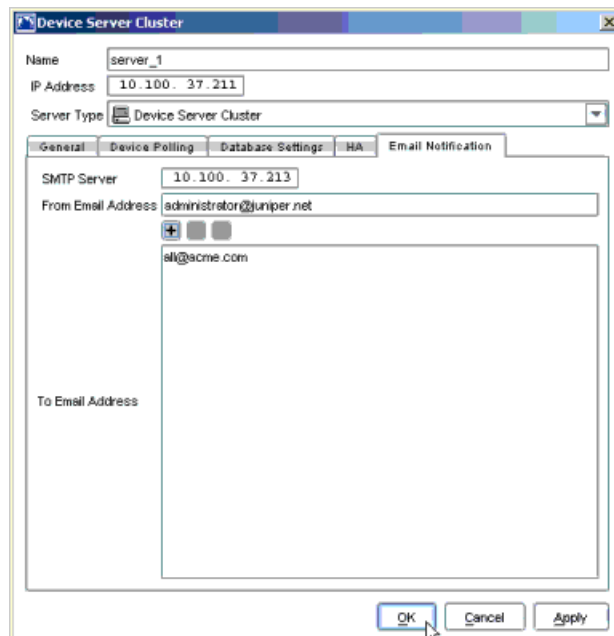
The screenshot shows the 'Device Server Cluster' configuration window with the 'HA' tab selected. The 'Name' field is 'server_1' and the 'IP Address' is '10.100.37.211'. The 'Server Type' is set to 'Device Server Cluster'. The 'General' tab is active, showing the 'IP Address of Secondary Server' as '10.100.37.212'. The 'Secondary Device Server Manager Port' is empty. There is a 'Backup MP' section with a plus button and two minus buttons. Below this is a table with two columns: 'Mapped IP Address of Secondary Server' and 'Mapped Port of Secondary Server'. The first row shows '0.0.0.0' and '7800'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Mapped IP Address of Secondary Server	Mapped Port of Secondary Server
0.0.0.0	7800

4. Click **Apply** when you are done.
5. (Optional) Click to activate the **Email Notification** tab. Configure the following parameters as shown in [Figure 10 on page 124](#):

- a. Enter the IP Address of the SMTP Server.
- b. Enter the e-mail address referenced in the e-mail notification in the **From Email Address** field.
- c. Click the plus + button to add recipients of the e-mail notification. The **New Add/Edit E-mail Address** window appears enabling you to enter an e-mail address. Click **OK** when you are done.

Figure 10: Configuring e-mail Notification



- d. Click to select an e-mail address entry from the **To Email Address** list and click on the **Edit** button to edit the e-mail address.
 - e. Click the minus - button to remove recipients of the e-mail notification.
6. Click **Apply** when you are done.

Installing NSM In an Extended HA Configuration

If you are installing the management system in an extended configuration (GUI server and Device Server on separate server machines) with HA enabled, you will need to run the management system installer on four separate server machines:

1. Primary GUI server
2. Secondary GUI server
3. Primary Device server
4. Secondary Device server

Use the system parameters referred to in “[Extended HA Configuration Parameters](#)” on [page 91](#) to configure HA on both servers. If you are using a shared disk, you will also need to configure the system parameters referred to in “[Shared Disk Parameters](#)” on [page 92](#).

After installing the primary management system and secondary management system, you will need to use the UI to configure the HA cluster. Finally, we recommend that you test the initial replication process.



NOTE: If you are installing NSM for the first time on a Solaris server, you must reboot the server after installation.

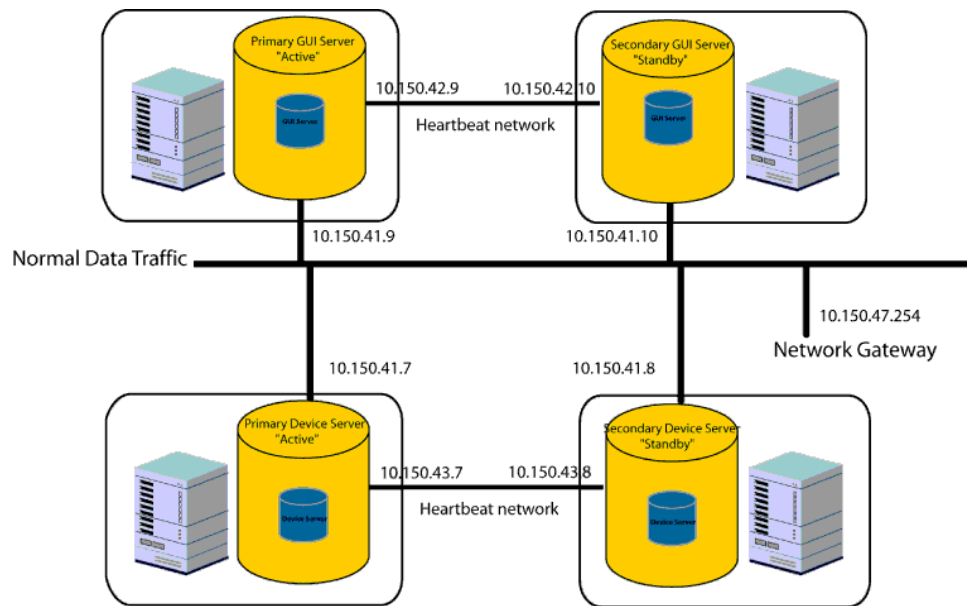
Example: Installing NSM in an Extended HA Configuration

For example, install the management system in an extended HA configuration (GUI server and Device Server on separate server machines) with the following parameters:

- No shared disk
- No Statistical Report Server
- Only one heartbeat link between the primary/secondary servers
- IP Address of the primary GUI server is 10.150.41.9
- IP Address of the secondary GUI server is 10.150.41.10
- IP Address of the primary Device Server is 10.150.41.7
- IP Address of the secondary Device Server is 10.150.41.8
- IP Address outside the HA Cluster is 10.150.47.254
- Daily local database backup
- No daily remote database backup
- Heartbeat link sent over remote replications/backups

[Figure 11 on page 126](#) depicts the configuration example above:

Figure 11: Extended HA Configuration Example



The NSM installer script output for the primary GUI server installations follows.

Primary GUI Server Installation Script

The following example shows the complete installer script output for installing the primary GUI server:

```
[root@h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
```

```

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 2

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]>
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### GUI SERVER SETUP DETAILS #####

Will the GUI Server data directory be located on a shared disk partition? (y/n)
[n]>

The GUI Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/GuiSvr. Because
the user data (including database data and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/GuiSvr]>

The GUI Server stores all of the database logs under a single directory.
By default, this directory is /var/netscreen/GuiSvr/xdm/log. Because
the database log can grow to be quite
large, it is sometimes desirable to place this log in another
partition.
Please enter an alternative location for this log if
so desired, or press ENTER for the location specified in the
brackets.
Enter database log directory location [/var/netscreen/GuiSvr/xdm/log]>

Enter the management IP address of this server [10.150.41.9]>

Enter the https port for NBI service [8443]>

Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter the one-time password for this Gui Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

```

```
Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

CFM password for user 'cfmuser'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>
Enter the same password again for CFM user
Changing password for user cfmuser.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the IP address for the primary HA Server [10.150.41.9]>

Enter the IP address for the secondary HA Server []> 10.150.41.10

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.9]>
10.150.42.9

Enter the IP address for the peer's primary heartbeat link [10.150.41.10]>
10.150.42.10

Enter the IP address that will be used for remote HA replications [10.150.41.10]>

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter an IP address outside of the cluster []> 10.150.47.254

Enter the rsync replication timeout [3600]>
```

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.

Please reset the trust relationship with 'nsm' user.

Here are sample commands:

```
cd /home/nsm
```

```
su nsm
```

```
ssh-keygen -t rsa
```

```
chmod 0700 .ssh
```

```
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys
```

BACKUP SETUP DETAILS

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm ...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

POST-INSTALLATION OPTIONS

Start High Availability daemon processes when finished? (y/n) []> n

CONFIRMATION

About to proceed with the following actions:

- Install GUI Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine will have base license with maximum 25 devices
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdm/log
- Use IP address 10.150.41.9 for management
- Use port 8443 for NBI Service
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- IP address for the primary HA Server: 10.150.41.9
- IP address for the secondary HA Server: 10.150.41.10
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.42.9
- IP address for the peer's primary heartbeat link: 10.150.42.10

- IP address for remote HA replications: 10.150.41.10
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n)> y

PERFORMING INSTALLATION TASKS

----- INSTALLING GUI Server -----

```
Looking for existing RPM package.....ok
Removing existing GUI Server RPM.....ok
Installing GUI Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in GUI Server config file(s).....ok
Setting permissions for GUI Server.....ok
Running generateMPK utility.....ok
Running fingerprintMPK utility.....ok
Installation of GUI Server complete.
```

----- INSTALLING HA Server -----

```
Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.
```

----- SETTING START SCRIPTS -----

```
Disabling GUI Server start script.....ok
Enabling HA Server start script.....ok
```

PERFORMING POST-INSTALLATION TASKS

```
Converting GuiSvr SetDB to XDB .....ok
Loading GuiSvr XDB data from init files .....ok
ok
Running webproxy Cert Generation.....ok
Removing staging directory.....ok
```

NOTES:

- Installation log is stored in
/usr/netscreen/GuiSvr/var/errorLog/netmgtInstallLog.20080902163033

```
- This is the GUI Server fingerprint:
1C:67:DF:06:51:A4:C4:5B:CF:A9:19:B4:BA:98:79:01:0C:F2:63:4F
You will need this for verification purposes when logging into the GUI
Server. Please make a note of it.

[root@C73-16 ~]#
```

Secondary GUI Server Installation

The following example shows the complete installer script output for installing the secondary GUI server:

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 2

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]> n
```

WARNING: The servers need to be stopped on the primary server during the installation of this software to avoid data corruption.

GUI SERVER SETUP DETAILS

Will the GUI Server data directory be located on a shared disk partition? (y/n) [n]>

The GUI Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/GuiSvr. Because the user data (including database data and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition.

Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

Enter data directory location [/var/netscreen/GuiSvr]>

The GUI Server stores all of the database logs under a single directory. By default, this directory is /var/netscreen/GuiSvr/xdb/log. Because the database log can grow to be quite large, it is sometimes desirable to place this log in another partition.

Please enter an alternative location for this log if so desired, or press ENTER for the location specified in the brackets.

Enter database log directory location [/var/netscreen/GuiSvr/xdb/log]>

Enter the management IP address of this server [10.150.41.10]>

Enter the https port for NBI service [8443]>

Please enter a password for the 'super' user

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

Enter the one-time password for this Gui Server

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

CFM password for user 'cfmuser'

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

Enter the same password again for CFM user

Changing password for user cfmuser.

New UNIX password:

BAD PASSWORD: it is based on a dictionary word

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

HIGH AVAILABILITY (HA) SETUP DETAILS

Enter the IP address for the primary HA Server []> 10.150.41.9

```

Enter the IP address for the secondary HA Server [10.150.41.10]>

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.10]>
10.150.42.10

Enter the IP address for the peer's primary heartbeat link [10.150.41.9]>
10.150.42.9

Enter the IP address that will be used for remote HA replications [10.150.41.9]>

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter an IP address outside of the cluster []> 10.150.47.254

Enter the rsync replication timeout [3600]>

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the
secondary server, via ssh-keygen, is a requirement for the
remote replication to work properly.
Please reset the trust relationship with 'nsm' user.
Here are sample commands:
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh

```

```
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

##### POST-INSTALLATION OPTIONS #####

Start High Availability daemon processes when finished? (y/n) []> n

##### CONFIRMATION #####

About to proceed with the following actions:
- Install GUI Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine will have base license with maximum 25 devices
- This machine participates in an HA cluster
- This server is the primary: No
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdm/log
- Use IP address 10.150.41.10 for management
- Use port 8443 for NBI Service
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- IP address for the primary HA Server: 10.150.41.9
- IP address for the secondary HA Server: 10.150.41.10
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.42.10
- IP address for the peer's primary heartbeat link: 10.150.42.9
- IP address for remote HA replications: 10.150.41.9
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: n
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n)> y
```

```

##### PERFORMING INSTALLATION TASKS #####

----- INSTALLING GUI Server -----
Looking for existing RPM package.....ok
Removing existing GUI Server RPM.....ok
Installing GUI Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in GUI Server config file(s).....ok
Setting permissions for GUI Server.....ok
Running generateMPK utility.....ok
Running fingerprintMPK utility.....ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Disabling GUI Server start script.....ok
Enabling HA Server start script.....ok

##### PERFORMING POST-INSTALLATION TASKS #####
Running webproxy Cert Generation.....ok
Removing staging directory.....ok

NOTES:
- Installation log is stored in
  /usr/netscreen/GuiSvr/var/errorLog/netmgtInstallLog.20080902165652

- This is the GUI Server fingerprint:
  3F:B6:8B:A6:E9:E6:02:06:F6:24:3A:C7:26:E7:2F:DD:3A:31:D4:84
  You will need this for verification purposes when logging into the GUI
  Server. Please make a note of it.

[root@C73-16 ~]#

```

Primary Device Server Installation

The following example shows the complete installer script output for installing the primary Device Server:

```

sh nsm2012.2_servers_linux_x86.sh
##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok

```

```

Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 1

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]>
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### DEVICE SERVER SETUP DETAILS #####

Will the Device Server data directory be located on a shared disk partition? (y/n)
[n]>

The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

Enter the ID assigned by the GUI to this Device Server (1-65535) []> 1

Enter the one-time password for this Device Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

```

```

To enable the Device Server to communicate with the GUI Server, you must
provide the IP address of the running GUI Server
Enter the IP address of the running GUI Server []> 10.150.41.9
##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the IP address for the primary HA Server [10.150.41.7]>

Enter the IP address for the secondary HA Server []> 10.150.41.8

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.7]>
10.150.43.7

Enter the IP address for the peer's primary heartbeat link [10.150.41.8]>
10.150.43.8

Enter the IP address that will be used for remote HA replications [10.150.41.8]>

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter an IP address outside of the cluster []> 10.150.47.254

Enter the rsync replication timeout [3600]>

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the
secondary server, via ssh-keygen, is a requirement for the
remote replication to work properly.

```

```

Please reset the trust relationship with 'nsm' user.
Here are sample commands:
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

##### DEVSVR DB SETUP DETAILS #####

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

##### POST-INSTALLATION OPTIONS #####

NOTE: Do not start up the Device Server unless you have already added it to
the system from the UI.
Start High Availability daemon processes when finished? (y/n) []> n

##### CONFIRMATION #####

About to proceed with the following actions:
- Install Device Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store Device Server data in /var/netscreen/DevSvr
- Connect to GUI Server at 10.150.41.9:7801
- IP address for the primary HA Server: 10.150.41.7
- IP address for the secondary HA Server: 10.150.41.8
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.43.7
- IP address for the peer's primary heartbeat link: 10.150.43.8
- IP address for remote HA replications: 10.150.41.8
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254

```

```

- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start High Availability daemon processes when finished: No

```

Are the above actions correct? (y/n)> y

PERFORMING INSTALLATION TASKS

----- INSTALLING Device Server -----

```

Looking for existing RPM package.....ok
Removing existing Device Server RPM.....ok
Installing Device Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in Device Server config file(s).....ok
Setting permissions for Device Server.....ok
----- Setting up PostgreSQL for DevSvr -----
Setting up PostgreSQL for DevSvr.....ok
Installation of Device Server complete.

```

----- INSTALLING HA Server -----

```

Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.

```

----- SETTING START SCRIPTS -----

```

Disabling Device Server start script.....ok
Enabling HA Server start script.....ok

```

PERFORMING POST-INSTALLATION TASKS

```

Running nacnCertGeneration.....ok
Running idpCertGeneration.....ok
Removing staging directory.....ok

```

NOTES:

```

- Installation log is stored in
/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20080902171434

```

[root@C73-16 ~]#

Secondary Device Server Installation

The following example shows the complete installer script output for installing the secondary Device Server:

```
[root@h ~]# sh nsm2012.2_servers_linux_x86.sh
##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) []> 1

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]> n
WARNING: The servers need to be stopped on the primary server
during the installation of this software to avoid data corruption.

##### DEVICE SERVER SETUP DETAILS #####

Will the Device Server data directory be located on a shared disk partition? (y/n)
[n]>

The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
```

```

Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

Enter the ID assigned by the GUI to this Device Server (1-65535) []> 2

Enter the one-time password for this Device Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

To enable the Device Server to communicate with the GUI Server, you must
provide the IP address of the running GUI Server
Enter the IP address of the running GUI Server []> 10.150.41.10
##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the IP address for the primary HA Server []> 10.150.41.7

Enter the IP address for the secondary HA Server [10.150.41.8]>

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
The IP addresses entered here must be correct and match on both ends of
the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.8]>
10.150.43.8

Enter the IP address for the peer's primary heartbeat link [10.150.41.7]>
10.150.43.7

Enter the IP address that will be used for remote HA replications [10.150.41.7]>

Enter the port used for heartbeat communication [7802]>

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter an IP address outside of the cluster []> 10.150.47.254

Enter the rsync replication timeout [3600]>

```

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.

Please reset the trust relationship with 'nsm' user.

Here are sample commands:

cd /home/nsm

su nsm

ssh-keygen -t rsa

chmod 0700 .ssh

-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

BACKUP SETUP DETAILS

Will this machine require local database backups? (y/n) [y]>

Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm
...)[02]>

Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

Enter the rsync backup timeout [3600]>

DEVSVR DB SETUP DETAILS

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [nsm]>

Enter Postgres DevSvr Db password for user 'nsm'

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

POST-INSTALLATION OPTIONS

NOTE: Do not start up the Device Server unless you have already added it to the system from the UI.

Start High Availability daemon processes when finished? (y/n) []> n

CONFIRMATION

About to proceed with the following actions:

- Install Device Server
- Install High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine participates in an HA cluster
- This server is the primary: No
- Store Device Server data in /var/netscreen/DevSvr

```

- Connect to GUI Server at 10.150.41.10:7801
- IP address for the primary HA Server: 10.150.41.7
- IP address for the secondary HA Server: 10.150.41.8
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.43.8
- IP address for the peer's primary heartbeat link: 10.150.43.7
- IP address for remote HA replications: 10.150.41.7
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: n
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start High Availability daemon processes when finished: No

```

Are the above actions correct? (y/n)> y

PERFORMING INSTALLATION TASKS

```

----- INSTALLING Device Server -----
Looking for existing RPM package.....ok
Removing existing Device Server RPM.....ok
Installing Device Server RPM.....ok
Installing JRE.....ok
Installing GCC.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in Device Server config file(s).....ok
Setting permissions for Device Server.....ok
----- Setting up PostgreSQL for DevSvr -----
Setting up PostgreSQL for DevSvr.....ok
Installation of Device Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package.....ok
Removing existing HA Server RPM.....ok
Installing HA Server RPM.....ok
Creating var directory.....ok
Putting NSROOT into start scripts.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Disabling Device Server start script.....ok
Enabling HA Server start script.....ok

```

```
##### PERFORMING POST-INSTALLATION TASKS #####
Running nacnCertGeneration.....ok
Running idpCertGeneration.....ok
Removing staging directory.....ok

NOTES:
- Installation log is stored in
/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20080902172929

[root@C73-16 ~]#
```

Next Steps

Now that you have completed installing the NSM management system with HA enabled, you are ready to begin managing your network. Refer to the *Network and Security Manager Administration Guide* and *Network and Security Manager Online Help* for information describing how to plan and implement NSM for your network.

CHAPTER 5

Upgrading to NSM 2012.2 from an Earlier Version

This chapter describes how to upgrade the management system and User Interface to Network and Security Manager (NSM) 2012.2. Upgrading includes patching the management system, upgrading the User Interface on your Windows or Linux client, and validating that you have upgraded successfully.



WARNING: The upgrade procedure described in this chapter is applicable only for NSM servers, and not for NSM Appliances.

This chapter contains the following sections:

- [Upgrade Overview on page 145](#)
- [PostgreSQL Database Upgrade from 8.1.7 to 8.4.10 on page 146](#)
- [Defining System Parameters on page 149](#)
- [Prerequisite Steps on page 154](#)
- [Upgrading NSM in a Standalone Configuration on page 158](#)
- [Upgrading the User Interface on page 170](#)
- [Upgrading NSM in a Distributed Configuration on page 171](#)
- [Upgrading NSM with HA Enabled on page 180](#)
- [Restoring Data if the Upgrade Fails on page 188](#)
- [Next Steps on page 188](#)

Upgrade Overview

The following procedure summarizes the process for upgrading NSM for most typical cases:

1. Define system parameters that you need to provide during the installation process.
2. Perform prerequisite steps. We recommend that you back up all your data files before you begin the upgrade process.

3. Download the NSM management system and User Interface installer software from the [Juniper Networks Web site](#).
4. Run the NSM management system installer on the system where the management system is currently installed. Specify that you want to upgrade both the GUI server and Device Server.
5. Upgrade the User Interface.
6. Launch the User Interface, then connect it to the management system.
7. Validate that you have successfully installed the management system and User Interface.

PostgreSQL Database Upgrade from 8.1.7 to 8.4.10

To resolve some database vulnerabilities in earlier releases of NSM, PostgreSQL support in NSM 2012.2. The PostgreSQL package is part of the system update process; before you can run the NSM installer to migrate to NSM 2012.2, you must run the system update script to updatehas been upgraded from version 8.1.7 to 8.4.10 PostgreSQL.



NOTE: The PostgreSQL upgrade process deletes existing data. PostgreSQL data must be backed up before the PostgreSQL upgrade and restored following the NSM upgrade. The system update script and NSM installer script have been modified to perform the PostgreSQL data backup and restore operations.

Upgrading PostgreSQL and Migrating to NSM 2012.2

Perform the following steps to migrate to NSM 2012.2:

- Run the 2012.2 system update script to upgrade the PostgreSQL package to 8.1.7. For more information, see “[System Update](#)” on page 146.
- Run the NSM installer to migrate to NSM release 2012.2. To know more about migrating to NSM release 2012.2, see “[Migrate NSM to 2012.2 NSM Release](#)” on page 147.

System Update

The system update script for NSM 2012.2 can back up existing PostgreSQL data. You will be prompted to choose to have the data backed up along with the location where the backup data will be stored. The default directory is **DevSvr var** and the default path is **/var/netscreen/DevSvr**.

If errors occur during the system update, the error log is created in the /tmp directory with the filename **system_update_2012.2_<timestamp>**. The update script as shown in [Figure 12 on page 147](#):

Figure 12: Update Script

```
[root@nsm-b11-vm1 es4_2012.1]# sh rhes4_new.sh

WARNING: This system update comes with an updated PostgreSQL database
packages, which requires a PostgreSQL Database backup to be taken.
Without backup and restore the postgresql data (application profiler data) will be lost

Do you want to take backup of the existing NSM PostgreSQL database : {Y}/N ?

Enter base directory location for management servers [/usr/netscreen] >

Please enter an alternative location for postgres backup data if
so desired, or press ENTER for the location specified in the brackets
Enter data directory location [/var/netscreen/devSvr] >

##### PERFORMING PGSQL BACKUP TASKS #####

Checking for sufficient disk space.....OK
Checking Device Server Status.....OK
Performing PostgreSQL DB Backup operation.....OK

##### PERFORMING SYSTEM UPDATE TASKS #####

Installing System Update for RedHat Enterprise Server 4.0 (Update 6)
warning: chkfontpath-1.10.0-2.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
warning: postgresql-8.4.10-1PGDG.rhel4.i386.rpm: V3 DSA signature: NOKEY, key ID 442df0f8
Preparing... ##### [100%]
 1:xorg-x11-font-utils ##### [ 3%]
 2:chkfontpath ##### [ 6%]
 3:ttmkfdir ##### [ 8%]
 4:xorg-x11-xauth ##### [11%]
 5:cpp ##### [14%]
 6:xorg-x11 ##### [17%]
 7:compat-libstdc++-296 ##### [19%]
 8:compat-libstdc++-33 ##### [22%]
 9:desktop-file-utils ##### [25%]
10:fontconfig ##### [28%]
11:fonts-xorg-100dpi ##### [31%]
12:fonts-xorg-75dpi ##### [33%]
13:fonts-xorg-base ##### [36%]
14:fonts-xorg-truetype ##### [39%]
15:freetype-devel ##### [42%]
16:pkgconfig ##### [44%]
```



NOTE: The system update files for Linux and Solaris are available on the [Software download](#) page.

Migrate NSM to 2012.2 NSM Release

The NSM 2012.2 installer can restore PostgreSQL data during the DevSvr upgrade operation. You will be prompted to choose to have the data restored and to enter the backup file path, as shown in [Figure 13 on page 148](#). The upgrade confirmation message is, as shown in [Figure 14 on page 148](#).

Figure 13: Installer Script

```

2) Upgrade both Device Server and GUI Server from 2010.4 to 2012.1
Enter selection (1-2) [2]> 2

WARNING:
You are about to upgrade the server on this machine. If you need to
backup your data before continuing, abort upgrade, backup your existing
data, and then rerun this upgrade.
Please see http://kb.juniper.net/KB3603 for details.

Hit Ctrl-C to abort upgrade or ENTER to continue

Do you want to do NSM installation with base license? (y/n) [y]>

Number of Devices managed by NSM is: 0
Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

Do you want to restore PostgreSQL database?(y/n) [y]>
Enter PostgreSQL data backup file location [/var/netscreen/DevSvr] /tmp
##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]>
==> Set to n

##### DEVICE SERVER SETUP DETAILS #####

##### GUI SERVER SETUP DETAILS #####

```

Figure 14: Upgrade Confirmation Message

```

##### CONFIRMATION #####

About to proceed with the following actions:
- Upgrade Device Server
- Upgrade GUI Server
- Upgrade High Availability Server
- This machine will have base license with maximum 25 devices
- Store base directory for management servers as /usr/netscreen
- Restore PostgreSQL Database :Yes
- PostgreSQL data backup file location: /tmp
- This machine does not participate in an HA cluster
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- Servers will not be restarted automatically
- Local database backups are disabled
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start server(s) when finished: No

Are the above actions correct? (y/n)> y

##### PERFORMING INSTALLATION TASKS #####

```

Using SQL Tools

The following tools are available for migrating PostgreSQL data:

- `pgSqlDbExporter.sh`— Used to export profiler data to the specified SQL file: `# sh pgSqlDbExporter.sh <file path>`, for example, `#sh pgSqlDbExporter.sh /tmp/pgSqlDump.sql`.
- `pgSqlDbImporter.sh`— Used to import SQL formatted profiler data into the profiler database `#sh pgSqlDbImporter.sh <file path>`, for example, `#sh pgSqlDbImporter.sh /tmp/pgSqlDump.sql`.

Defining System Parameters

During the upgrade process, you can choose to reconfigure the servers on which you want to upgrade NSM. If you choose to do so, you will be prompted to enter common system parameters such as passwords, port selection, and backup details. We recommend that you define these system parameters before performing the management system upgrade.

Ignore this section if you choose to keep the same configuration.

Standalone Configuration Parameters

Table 16 on page 149 identifies the system parameters that you need to identify if you are upgrading a standalone configuration of the management system — both GUI server and Device Server on the same server machine.

Table 16: Standalone Configuration—System Parameters

Parameter	Description	Your Value
Device Server data directory	<p>Directory location on the Device Server where device data is stored. Because the data on the Device Server can grow to be large, consider placing this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the Device Server stores data in:</p> <p><code>/var/netscreen/DevSvr/</code></p> <p>CAUTION: Do not place your data directory in <code>/usr/netscreen</code>. That path normally contains binary files and should not be used for data.</p>	
GUI Server data directory	<p>Directory location on the GUI server where user data is stored. Because the data on the GUI server can grow to be large, consider placing this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI server stores data in:</p> <p><code>/var/netscreen/GuiSvr/</code></p> <p>CAUTION: Do not place your data directory in <code>/usr/netscreen</code>. That path normally contains binary files and should not be used for data.</p>	

Table 16: Standalone Configuration—System Parameters (continued)

Parameter	Description	Your Value
Management IP address	<p>The IP address used by the running GUI server.</p> <p>The default is the IP address of the machine that you are installing on.</p>	
https port	The port number for listening for messages from the NSM API. The range is from 1025 through 65535. The default value is 8443.	
Initial “super” user password	The password required to authenticate the initial user in the system. By default, the initial superuser account receives all administrative privileges in the system.	
One-time GUI server password	A password that authenticates the server to its peers in a high-availability configuration, or authenticates a regional server with a central manager.	
Configuration file management password	Configures a user and password for NSM to perform configuration file management operations, and a corresponding UNIX user and password. The NSM and UNIX passwords must be identical.	
Local database backup directory	<p>Directory location where local database backup data is stored.</p> <p>By default, the GUI server stores local database backup data at:</p> <p><code>/var/netscreen/dbbackup/</code></p>	
Path to the rsync utility executable file	<p>Path to the rsync utility executable file.</p> <p>The default path is:</p> <p><code>/usr/bin/rsync</code></p>	
Remote Backup Machine IP Address	<p>IP address of the machine where remote backups are sent.</p> <p>By default, the NSM installer sets this to the IP address of the secondary HA Server.</p>	
Hour of the Day to Start Local Database Backup	<p>Time of day that you want the GUI server to backup the database. Type a 2 digit number representing the time of day in a 24 hour clock notation (00 through 23). For example, if you want the backup to begin at 4:00 AM, type 04; if at 4:00 PM, type 16. We recommend that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI server completes the daily backup process within the hour specified every day.</p> <p>By default, the GUI server performs the daily backup within an hour after 2 AM.</p>	

Table 16: Standalone Configuration—System Parameters (continued)

Parameter	Description	Your Value
Number of Local Database Backup Files Stored	Total number of database backup files that the GUI server stores. When the GUI server reaches the maximum number of backup files you configure, it overwrites the oldest file. By default, the GUI server stores seven backup files.	

Distributed Configuration Parameters

Table 17 on page 151 describes additional system parameters that you need to identify if you are upgrading a distributed configuration of the management system — GUI server and Device Server on separate server machines:

Table 17: Distributed Configuration — System Parameters

Parameter	Description	Your Value
Device Server ID	Unique ID assigned when you add the Device Server.	
Password for GUI Server Connection	Password assigned to the Device Server enabling it to authenticate with the GUI server when attempting to connect.	

HA Configuration Parameters

Table 18 on page 151 describes the system parameters that you need to identify if you are upgrading a standalone configuration of the management system with HA enabled:

Table 18: HA Configuration — System Parameters

Parameter	Description	Your Value
Primary HA Server IP address	IP address of the primary server participating in the HA cluster.	
Secondary HA Server IP address	IP address of the secondary server participating in the HA cluster.	
HA replications	Time interval with which you want the GUI server to replicate the database. By default, the GUI server replicates the database every 60 minutes.	
Heartbeat links between primary and secondary machine	Number of heartbeat communication paths between the primary and secondary machine. By default, only one communication link exists between the primary and secondary machines.	

Table 18: HA Configuration — System Parameters (continued)

Parameter	Description	Your Value
Shared password for heartbeat authentication.	Password that is required to authenticate heartbeat messages between the primary and secondary HA servers.	
IP Address for Primary machine's heartbeat link	IP address used for heartbeat communications on the primary server machine.	
Port used for heartbeat communication	The port number used for heartbeat communications. The default port is 7802.	
Heartbeat messages time interval	Time interval (in seconds) between heartbeat messages. The default is 15 seconds.	
Missing heartbeats before switchover occurs	Number of missing heartbeat messages before automatic switchover to the secondary machine occurs. The default is 4 messages.	
IP Address outside the HA cluster	Network IP Address used to monitor this server's network connection.	
HA directory	Directory location where high availability data is stored. Note that the same directory location is used if you configure this machine to perform local database backups. By default, the HA Server stores data at: /var/netscreen/dbbackup/	
Path to the rsync utility executable	Path to the rsync utility executable. The default path is: /usr/bin/	
Remote Backup Machine IP Address	IP address of the machine where remote backups are sent. By default, the NSM installer sets this to the IP address of the secondary HA Server.	

Table 18: HA Configuration — System Parameters (continued)

Parameter	Description	Your Value
Hour of the Day to Start Local Database Backup	<p>Time of day that you want the GUI server to backup the database. Type a 2 digit number representing the time of day in a 24 hour clock notation (00 through 23). For example, if you want the backup to begin at 4:00 AM, type 04; if at 4:00 PM, type 16. We recommend that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI server completes the daily backup process within the hour specified every day.</p> <p>By default, the GUI server performs the daily backup within an hour after 2 AM.</p>	
Number of Local Database Backup Files Stored	<p>Total number of database backup files that the GUI server stores. When the GUI server reaches the maximum number of backup files you configure, it overwrites the oldest file.</p> <p>By default, the GUI server stores seven backup files.</p>	

Shared Disk Parameters

Table 19 on page 153 identifies the additional system parameters that you need to identify to upgrade the management system with HA enabled with access to a shared disk:

Table 19: Shared Disk Parameters

Parameter	Description	Your Value
Command to mount the shared disk partition	<p>The command to mount the shared data partition.</p> <p>The default command is:</p> <p>/bin/mount /var/netscreen/DevSvr</p>	
Command to unmount the shared disk partition	<p>The command to unmount the shared data partition. Before configuring this command, you must first verify that your mounts are defined properly.</p> <p>The default command is:</p> <p>/bin/umount /var/netscreen/DevSvr</p>	
Command to check the integrity of the shared data partition	<p>The command to check the integrity on the shared data partition.</p> <p>The default command is:</p> <p>/sbin/fsck</p>	
Directory path for the shared disk	Directory path of the shared disk mount point.	

Prerequisite Steps

You can upgrade the management system from any previous running version of NSM.

Before you install the management system, you need to perform the following prerequisite steps:

1. Using your current version of NSM, upgrade any devices running ScreenOS 4.0.x or earlier version or remove them from your managed network. ScreenOS devices must run ScreenOS 5.0 or later version to be managed by NSM 2008.1 or later release. The NSM installer stops with errors if ScreenOS 4.0.x devices are present in the NSM database.
2. Ensure that the NSM appliance is accessible through a Serial Console
3. Log in to the appliance as root.

If you are already logged in as a user other than root, then run the following command to become root:

```
su
```

At the password prompt, enter the root password for the appliance.



NOTE: Although the management system runs with nsm user permissions, you must have root permissions to run the NSM installer.

4. Partition drives for sufficient disk space to accommodate your planned data requirements. Ensure that you have allocated a maximum amount of disk space for the data partition (/ partition).

See [“Hardware Recommendations” on page 283](#) for more information about the disk space requirements appropriate for your specific network.
5. Perform a backup of all files on the Device Server and GUI server. See [“Archiving and Restoring Logs and Configuration Data” on page 258](#) for more information archiving your data files.
6. Run the system update utility for your appropriate platform to ensure that you have all the up to date utilities and packages required to run the NSM installer properly. See [“Running the System Update Utility” on page 155](#) for more information on running the system update utility.
7. Configure shared memory size on your appropriate platform. See [“Configuring Shared Memory Size” on page 155](#) for more information.
8. Increase the rsync backup timeout and rsync replication timeout values to 3600. See [“Setting the rsync Timeout Values” on page 156](#).
9. If you are upgrading NSM on a Solaris server, ensure that all required locales have been installed and that the necessary edits to the `/etc/default/init` files have been made. See [“Preparing a Solaris Server for NSM” on page 157](#) for details.

Running the System Update Utility

Use the system update utility to upgrade your system with the latest patches and packages required to run the NSM management system installer properly.



NOTE: The NSM 2012.2 system update utility is compatible with Red Hat Enterprise Linux 4.0 Update 5 or version 5.0.

To run the system update utility:

1. Copy the system update utility appropriate for your platform from the NSM Installation directory to a suitable directory on the server.

We recommend that you save the utility in the `/usr` subdirectory.

2. Uncompress the system update utility file using the **gzip** command. For example:

```
gzip -d nsm2012.2-systemupdate-linuxES_5.tar.gz
```

3. Uncompress the appropriate system update utility **.tar** file. For example:

```
tar xfv nsm2012.2-systemupdate-linuxES_5.tar
```

A subdirectory for the platform ("es4", "es5", or "sol10") is created and all of the files required to update your system packages and utilities are extracted into that directory.

4. Navigate to the subdirectory.
5. Run the update shell archive script. For example, you can execute the shell archive script by running the following command:

```
<platform>.sh
```

For example, on Linux es4, the update script is named **rhes4_upd3.sh** and located in the **es4** directory.

For Solaris, the **systemupdate-solarisplatform.tar** file expands to `<platform>` and the update script is put in that directory. The script for Solaris is located in the same directory as the tar file. The name of the update script for Solaris is **update_solaris10.sh**.

The script proceeds to check your system for required updates. It next prompts you to press Enter to continue or Ctrl-C to stop.

6. Press Enter to continue. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 10 minutes depending upon the number of packages that need to be installed.

Configuring Shared Memory Size

Both the GUI and Device Server require that you modify the operating system shared memory in order to start and run.

On Solaris systems, you can do this by adding/updating the following in **/etc/system**:

```
set shmsys:shminfo_shmmax= 402653184
set shmsys:shminfo_shmmni=1
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256
set semsys:seminfo_semap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semml=32
```

On Linux systems, you can do this by adding/updating the following line in **/etc/sysctl.conf**:

```
kernel.shmmax= 402653184
```

After updating the shared memory requirements on your Linux or Solaris system, you must restart the server for your new settings to take effect.

Setting the rsync Timeout Values

The rsync values for backup timeout and replication timeout were set in previous releases to 1800 by default. To allow time to transfer the larger schema files in release 2010.2 and later releases, you must increase these values to 3600. To increase the rsync backup timeout and rsync replication timeout values, follow these steps:

1. Navigate to the High Availability configuration directory. For example:

```
cd /usr/netscreen/HaSvr/var/
```

2. Open the High Availability configuration file (**haSvr.cfg**) in any text editor.
3. To modify the rsync timeout values, configure the following parameters:

```
highAvail.rsyncCommandBackupTimeout=3600
highAvail.rsyncCommandReplicationTimeout=3600
```

4. Save the file.

Increasing Shared Memory Segment Maximum Size

If you are installing the management system on Solaris, we recommend that you increase the maximum size of your shared memory segment.

To increase the maximum size of shared memory:

1. Open the **/etc/system** file in any text editor.
2. Edit the OS kernel parameters by adding the following lines.

```
set shmsys:shminfo_shmmax=402653184
set shmsys:shminfo_shmmni=1
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256
set semsys:seminfo_semmap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semmsl=32
```

3. Save the file.
4. Restart your system.

Preparing a Solaris Server for NSM

Perform these steps if you plan to upgrade NSM on a Solaris 10 server:

1. Install required locale files.

Use the following command to check which locale files are currently installed:

```
/usr/bin/locale -a
```

Ensure that the following locales are installed. If you have all required locales, proceed to Step 2.

```
C
POSIX
en_CA
en_CA.IS08859-1
en_CA.UTF-8
en_US
en_US.IS08859-1
en_US.IS08859-15
en_US.IS08859-15@euro
en_US.UTF-8
es
es.UTF-8
es_MX
es_MX.IS08859-1
es_MX.UTF-8
fr
fr.UTF-8
fr_CA
fr_CA.IS08859-1
fr_CA.UTF-8
iso_8859_1
```

Use the Solaris 10 installation DVD to load any missing locales. The minimum supported Solaris 10 revision is 6/06. You can download the DVD from www.sun.com. Mount the DVD (in this example, `/solaris`) and issue the following commands:

```
/usr/sbin/pkgadd -d /solaris/Solaris_10/Product SUNWladm
```

```
/usr/sbin/localeadm -a en_US -d /solaris/Solaris_10/Product
```

2. Edit the `/etc/default/init` file to include the following lines:

```
LC_COLLATE=en_US.UTF-8
LC_CTYPE=en_US.UTF-8
LC_MESSAGES=C
LC_MONETARY=en_US.UTF-8
LC_NUMERIC=en_US.UTF-8
LC_TIME=en_US.UTF-8
```

3. Reboot the Solaris server.

```
/usr/sbin/reboot
```

Upgrading NSM in a Standalone Configuration

To upgrade to NSM 2012.2 on a standalone system:

1. Load the NSM installer software onto the server where the NSM management system is currently installed. You can download the NSM installer from the [Juniper Networks Web site](#).
2. Navigate to the directory where you saved the management system installer file (typically the `/var/tmp/` subdirectory).
3. Run the management system installer.

On Linux, run the following command:

```
sh nsm2012.2_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2012.2_servers_sol_sparc.sh
```

The installation begins automatically by performing a series of preinstallation checks. The NSM installer ensures that:

- The OS version and specified architecture are compatible.
- You are installing the correct software for your operating system.
- No ScreenOS 4.0.x or earlier release devices exist in the database.

If the NSM installer discovers ScreenOS 4.0.x or earlier devices in the network, the NSM installer fails with the following message:

```
Device(s) running ScreenOS 4.0.x or earlier release were found in the managed
network.
Using your currently installed version of NSM, upgrade all such devices to
ScreenOS 5.0 or later version
or remove them from the network, and then rerun the installer.
```

- All of the needed software binaries and packages are present.

If any component is missing, the NSM installer displays a message identifying the missing component:

```
Checking for platform-specific packages.....FAILED
The Following list of Packages are Required for NSM installation.
Please install the system update utility before continuing.
chkfontpath
```

- You have the correct version of the PostgreSQL database.
- You have correctly logged in as root and that the nsm user exists. The NSM installer creates the nsm user, if it does not already exist.
- For Linux servers, the NSM installer checks whether iptables is running. If not, then the NSM installer continues.

If iptables is running, the NSM installer displays a message similar to the following:

```
Checking for iptables service.....ok
Iptables is found to be running on the system. Please make sure the ports
7801 7802, 443, 7800, 7804 are open and available for NSM to run.

Please press enter to continue:
```

Ensure the required ports for NSM are available before continuing.

- The system has sufficient disk space and RAM.

The NSM installer stops any running servers.



NOTE: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the NSM installer successfully performed a task.
- “OK” indicates that the NSM installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the NSM installer performed a task or check, but it was not successful. See the install log for information about the failure. This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of the install, the log might be in `/var/tmp`.

The NSM installer performs some preinstallation checks:

```
##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking if ScreenOS 4.0.x or earlier device in network....ok
Checking for CPU architecture.....ok
```

```

Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if installed Device Server is newer.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

```

The NSM installer extracts the software payloads and prompts you to install NSM with the base license.

```

##### EXTRACTING PAYLOADS #####
Extracting payload.....ok
Decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
Checking device count.....ok

Do you want to do NSM installation with base license? (y/n) [y]> n

```

4. For a base license installation—that is, one that does not require the license key file—enter **y**.

For an installation that requires a license key file, enter **n**. You will enter the licence file path later. See [“Introduction” on page 3](#) for information about obtaining license keys.

The NSM installer prompts you to specify the components that you want to install.

```

1) Clean install of both Device Server and GUI Server
2) Refresh both Device Server and GUI Server
Enter selection (1-2) [2]> 2

```



NOTE:

- For upgrades to major release versions, the NSM installer displays the **Upgrade** option instead of the **Refresh** option. For example, if you upgrade from NSM 2010.3 to NSM 2012.2, the NSM installer displays the **Upgrade** option.
- For upgrades to minor release versions, the NSM installer displays the **Patch** option instead of the **Refresh** option. For example, if you upgrade from NSM 2012.2R1 to NSM 2012.2R5, the NSM installer displays the **Patch** option.

5. Type **2** to refresh the Device Server and the GUI server.



CAUTION: Selection 1 deletes the previous installation and all its data.

Upgrades between minor releases display the following prompt at this point:

```
Will server(s) need to be reconfigured during the refresh? (y/n) [n]>
```

To skip the configuration questions, enter **n**.

For upgrades between major releases, such as from 2008.1 to 2012.2, or if you enter **y** in response to the previous prompt, you will be prompted for configuration input.

The NSM installer prompts whether you want to enable FIPS support.

6. If you require FIPS support, enter **y**. Otherwise, press Enter to accept the default value.
7. To reconfigure the servers during the refresh, enter **y**.

To keep the same configuration, enter **n**.

If you choose to reconfigure the servers, you will later be prompted to re-enter system parameters.

What happens next depends on whether you selected to install with a base license or with a license key file. If you are installing with a base license, skip step 8.

8. If you chose to install a license key file, the NSM installer displays the installation ID of the system prompts you to enter the license key file path.

```
The installation ID for this system is: 3FFFEA90278AA
```

```
Number of Devices managed by NSM is: 23
```

```
Enter the License File Path>
```

- a. Use the installation ID to obtain a license key file from the LMS system and save it on your local drive as described in [\[Unresolved xref\]](#).
- b. Enter the license key file path.

The NSM installer validates the license key file.



NOTE: If the NSM installer prompts you for the license file and the license key is not available, press **Ctrl+Z** to exit the NSM installer.

9. Provide the following configuration information:
 - Whether this machine will participate in an HA cluster.
 - The GUI server one-time password.

- Whether you want to configure interoperability with NetScreen-Statistical Report Server.
- An NSM password and a UNIX password for configuration file management.



NOTE: The configuration file management passwords for NSM and for UNIX must be identical.

- Whether you want server processes restarted automatically if they fail.
- Backup details including time of day to take the backup, how many backups to keep, and whether to take a remote backup.



NOTE: You must allow local backup if you want to specify remote backup.

- Database server details including the port number, and password.

The NSM installer next prompts if you want to start the servers when finished.

10. To restart the servers when finished, enter **y**. If you do not want to restart server processes, enter **n**.



NOTE: When you restart your operating system, the GUI and Device Servers start automatically.

The NSM installer prompts you to verify your upgrade configuration settings.

11. Verify your settings. If the configuration settings are correct, enter **y** to proceed. If you enter **n**, the NSM installer returns to the previous prompt.

The upgrade proceeds automatically. The NSM installer proceeds to perform the following actions:

- Upgrades the Device server.
- Upgrades the GUI server.
- Installs the HA server.
- Sets start scripts.
- Performs postinstallation tasks such as removing the staging directory and starting the server processes (if configured).

Several messages display to confirm the installation progress. The NSM installer runs for several minutes, and then exits.

After the NSM installer finishes, it generates a log file with the output of the installation commands for troubleshooting purposes. The NSM installer indicates the name of the

installation log file and the directory location where it is saved. This file is saved by default in the **tmp** subdirectory.

The naming convention used for the installation log file is:

```
netmgtInstallLog.<current date><current time>
```

For example, if you ran the NSM installer on April 1, 2008 at 6:00 PM, then the installation log file would be named **netmgtInstallLog.20080401180000**.

Typical Output for a Standalone Upgrade

The following example upgrades a standalone installation using the base license and without reconfiguring server parameters.

```
[root@/h ~]# sh nsm2012.2_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if installed Device Server is newer.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
Checking device count.....ok

1) Clean install of both Device Server and GUI Server
2) Upgrade both Device Server and GUI Server from 2008.1r1 to 2011.1
Enter selection (1-2) [2]> 2

Do you want to do NSM installation with base license? (y/n) [y]>

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>
```

```
Number of Devices managed by NSM is: 0
##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]>
==> Set to n

##### DEVICE SERVER SETUP DETAILS #####

##### GUI SERVER SETUP DETAILS #####

==> Set GUI Server one-time password

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>
==> CFM user is set to 'cfmuser'

CFM password for user 'cfmuser'
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>
Enter the same password again for CFM user
Changing password for user cfmuser.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Automatic restarts of servers? (y/n) [y]>
==> Set to y

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>
==> Set to y

==> Setting start hour for database backup to 02

Will daily backups need to be sent to a remote machine? (y/n) [n]>
==> Set to n

Enter number of database backups to keep. The default value will keep the last
seven backups.
The oldest backup copy will be overwritten by the new backup copy [7]>
==> Set number of database backups to keep to 7

Enter the rsync backup timeout [3600]>
==> Set to 3600

Enter database backup directory [/var/netscreen/dbbackup]>
==> Setting database backup directory to /var/netscreen/dbbackup
WARNING: Directory /var/netscreen/dbbackup already exists.
Existing backups in this directory may not be
compatible with this new software.
Please exit installation and move the contents
as they will get WIPED OUT during installation.
```

```

##### DEVSVR DB SETUP DETAILS #####

==> Postgres DevSvr Db port set to 5432

==> Postgres DevSvr Db super user set to 'nsm'

==> Postgres DevSvr Db password set for 'nsm'

##### POST-INSTALLATION OPTIONS #####

Start server(s) when finished? (y/n) []> y

##### CONFIRMATION #####

About to proceed with the following actions:
- Upgrade Device Server
- Upgrade GUI Server
- Upgrade High Availability Server
- Store base directory for management servers as /usr/netscreen
- This machine will have base license with maximum 25 devices
- This machine does not participate in an HA cluster
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- Servers will be restarted automatically in case of a failure
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start server(s) when finished: Yes

Are the above actions correct? (y/n)> y

##### PERFORMING INSTALLATION TASKS #####

----- UPGRADING Device Server -----
ok
Upgrading DevSvr RPM.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Installing JRE.....ok
Installing GCC.....ok
----- Setting up PostgreSQL for DevSvr -----
Setting up PostgreSQL for DevSvr.....ok
Setting permissions for Device Server.....ok
Upgrade of DevSvr complete.

----- UPGRADING GUI Server -----
Copying data to the installer backup directory.....ok
ok
Upgrading GuiSvr RPM.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Installing JRE.....ok
Installing GCC.....ok
Adding Cfm.log.....ok

```

```

Adding Cfm.password.....ok
Running generateMPK utility.....ok
Running fingerprintMPK utility.....ok
Setting permissions for GUI Server.....ok
Upgrade of GuiSvr complete.

----- UPGRADING HA Server -----
Upgrading HaSvr RPM.....ok
Putting NSROOT into start scripts.....ok
Adding highAvail.isFailOverEnabled.....ok
Filling in HA Server config file(s).....ok
Setting permissions for HA Server.....ok
Upgrade of HaSvr complete.

----- SETTING START SCRIPTS -----
Enabling Device Server start script.....ok
Enabling GUI Server start script.....ok
Enabling HA Server start script.....ok

##### PERFORMING POST-INSTALLATION TASKS #####
ok
Loading GuiSvr XDB data from init files .....ok
Migrating GuiSvr data.....ok
ok
Removing staging directory.....ok
Starting GUI Server.....ok
Starting Device Server.....ok
Starting HA Server.....ok

NOTES:
- Installation log is stored in
/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20080904163031

- This is the GUI Server fingerprint:
9F:8C:02:85:69:74:86:0D:96:84:1C:79:F0:7D:6A:DC:51:A1:81:21
You will need this for verification purposes when logging into the GUI
Server. Please make a note of it.

[root@C73-16 ~]#

```

Installing NSM with an IPv6 Management Address

Beginning in NSM2012.2R10, NSM can be installed with an IPv6 management address for upgrading to NSM 2012.2.



NOTE:

- You must configure the IPv6 address in the NSM server before starting the installation.
- Existing devices with IPv4 addresses connect to the NSM server through a mapped IPv4 address (::ffff:192.168.1.1) and display the connection status as Up in the NSM GUI. Not all features function properly in this setting. We recommend that you activate existing devices with IPv6 addresses using the RMA workflow.

Typical Output for a Standalone Upgrade

```
[root@nsm-b3-vm7 ~]# sh nsm2012.2R10_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
WARNING:
Please make sure the following lines are present in the /etc/sysctl.conf file.
kernel.shmmax= 402653184
The install will exit if they aren't present. Please Reboot the system before
continuing
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if selinux is enabled.....ok
Checking if installed Device Server is newer.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
Checking device count.....ok

1) Clean install of both Device Server and GUI Server
2) Upgrade both Device Server and GUI Server from 2012.1R10 to 2012.2R10
Enter selection (1-2) [2]>

WARNING:
You are about to upgrade the server on this machine. If you need to
backup your data before continuing, abort upgrade, backup your existing
data, and then rerun this upgrade.
Please see http://kb.juniper.net/KB3603 for details.

Hit Ctrl-C to abort upgrade or ENTER to continue

Do you want to do NSM installation with base license? (y/n) [y]>

Number of Devices managed by NSM is: 0
Enter base directory location for management servers [/usr/netscreen]>
```

```

Enable FIPS Support? (y/n) [n]>

Do you want to restore PostgreSQL database?(y/n) [y]> n
Select Device Schema to be loaded in NSM

  1) Load all Device Family Schemas
  2) Load Screen OS Device Schema only (Screen OS)
  3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
Enter selection (1-3)[1]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]>
==> Set to n

##### DEVICE SERVER SETUP DETAILS #####

##### GUI SERVER SETUP DETAILS #####

Do you want to change Management IP address (y/n) ?[n]> y
Enter the type of management IP address of this server (4-IPv4 / 6-IPv6) [4]> 6
Enter the management IPv6 address of this server [fc00::10:205:1:95]>
==> Management IP set to fc00::10:205:1:95

Enter the https port for NBI service [8443]>

Enter the one-time password for this Gui Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

==> CFM password set for 'cfmuser'

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Automatic restarts of servers? (y/n) [n]>
==> Set to n

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [n]>
==> Set to n

##### DEVSVR DB SETUP DETAILS #####

==> Postgres DevSvr Db port set to 5432

==> Postgres DevSvr Db super user set to 'nsm'

==> Postgres DevSvr Db password set for 'nsm'

##### POST-INSTALLATION OPTIONS #####

```

```

Start server(s) when finished? (y/n) []> y

##### CONFIRMATION #####

About to proceed with the following actions:
- Upgrade Device Server
- Upgrade GUI Server
- Upgrade High Availability Server
- This machine will have base license with maximum 25 devices
- Store base directory for management servers as /usr/netscreen
- Restore PostgreSQL Database : No
- All Device Families Schemas Load
- This machine does not participate in an HA cluster
- Use IP address fc00::10:205:1:95 for management
- Use port 8443 for NBI Service
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- Servers will not be restarted automatically
- Local database backups are disabled
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start server(s) when finished: Yes

Are the above actions correct? (y/n)> y

```

Starting Server Processes Manually

If you did not specify the NSM installer to start the servers when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually, enter the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

If you start the HA Server process, then it automatically starts the GUI server and Device Server processes.

NSM processes always run with nsm user permissions, even if you have root permissions when you start them.

Validating Management System Status

If you specified that you want the NSM installer to start servers when finished, we recommend that you view the status of the HA, Device, and GUI Servers to confirm that all services are running.

To check the status of the HA Server process, enter the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh status
```

To check the status of the GUI server, enter the following command:

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh status
```

To check the status of the Device Server, enter the following command:

```
/usr/netscreen/DevSvr/bin/devSvr.sh status
```

See [“Controlling the Management System” on page 251](#) for more information on manual commands that you can send to the management system.

Upgrading the User Interface

For Release 2007.3 and later releases of the UI client, you can upgrade to the 2012.2 Release automatically. For earlier releases, you must manually download and install the new UI client.

- [Downloading and Installing the UI Client Automatically on page 170](#)
- [Downloading and Installing the UI Client Manually on page 170](#)
- [Validating the Upgrade on page 171](#)

Downloading and Installing the UI Client Automatically

To update an existing NSM Client that supports automatic downloading:

1. Connect to the server using the client. If your current client release version is incompatible with the server release version, a confirmation dialog box appears.
2. Click **Yes** to download the new client.
3. Select a local directory, name a file in which to save the new NSM Client, and then click **Select Save Directory for Installer**. The new client downloads automatically and starts the InstallAnywhere wizard.
4. Follow the directions in the wizard to complete the installation.
5. Connect to the server again using the new client. The NSM login dialog box appears.
6. Enter your username and password to establish a connection with the server.

Downloading and Installing the UI Client Manually

To download and install the UI client from the [Juniper Networks web site](#), follow the steps described in [“Installing the User Interface” on page 39](#).

The NSM User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based that meets minimum system requirements. The InstallAnywhere wizard guides you through all the steps required to configure and install the NSM UI.

Validating the Upgrade

After you have upgraded the management system and UI, we recommend that you validate basic information configured on the Device Server. You can use the Server Manager in the NSM UI to view and edit your configuration on the management system.

To validate your configuration on the Device Server:

1. From the NSM UI, select **Server Manager>Servers**. The Servers view appears displaying Device Server and GUI server information.
2. Click on the Device Server and click on the **Edit** icon or right-click on the Device Server and select **Edit** to view all information available on the Device Server.
3. Use the General tab to verify the following information:
 - Device Server Manager Port — the default port is 7800.
 - Device Server ID — the ID number identifies the Device Server; you cannot change the Device Server ID.
 - Mapped IP address — the IP address that is manually defined in the UI.



NOTE: You can configure the Device Server to use a Mapped IP (MIP) address. A MIP maps the destination IP address in an IP packet header to another static IP address, enabling the managed device to receive incoming traffic at one IP address, and automatically forward that traffic to the mapped IP address. MIPs enable inbound traffic to reach private addresses in a zone that contains NAT mode interfaces.

4. Click **OK** when you are done.

Upgrading NSM in a Distributed Configuration

The process for upgrading the management system on separate servers (in the distributed configuration) is as follows:

1. Perform the prerequisites steps described as if upgrading the management system in a standalone configuration.
2. Run the management system installer on the server where you have currently installed the GUI server. Specify that you want to upgrade the GUI server only.
3. Run the management system installer on the server where you have currently installed the Device Server. Specify that you want to upgrade the Device Server only.
4. Wait approximately 10 to 15 minutes so that the Device Server can successfully reconnect to the GUI server.
5. Upgrade the UI client on the computers where you have installed the UI client. See [“Upgrading the User Interface” on page 170](#) for details.
6. Launch the UI and verify that you can connect to the upgraded GUI server.

Installing NSM with IPv6 Management addresses

An example of the output for a typical distributed configuration is as follows:

- [Primary GUI Server Output on page 172](#)
- [Primary Dev Server Output on page 176](#)

Primary GUI Server Output

```
[root@nsm-b3-vm7 ~]# sh nsm2012.2R10_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
WARNING:
Please make sure the following lines are present in the /etc/sysctl.conf file.
kernel.shmmax= 402653184
The install will exit if they aren't present. Please Reboot the system before
continuing
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if selinux is enabled.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
Checking device count.....ok

1) Install Device Server, upgrade GUI Server from 2012.1R10 to 2012.2R10
2) Install Device Server, clean install GUI Server
3) Upgrade GUI Server only from 2012.1R10 to 2012.2R10
4) Clean install of GUI Server only
Enter selection (1-4) [3]>

WARNING:
You are about to upgrade the server on this machine. If you need to
backup your data before continuing, abort upgrade, backup your existing
data, and then rerun this upgrade.
Please see http://kb.juniper.net/KB3603 for details.

Hit Ctrl-C to abort upgrade or ENTER to continue
```

```

Do you want to do NSM installation with base license? (y/n) [y]>

Number of Devices managed by NSM is: 0
Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

Select Device Schema to be loaded in NSM

  1) Load all Device Family Schemas
  2) Load Screen OS Device Schema only (Screen OS)
  3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
Enter selection (1-3)[1]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [y]>
==> Set to y

Is this machine the primary server for the HA cluster? (y/n) [y]>
==> Set to y
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### GUI SERVER SETUP DETAILS #####

Will the GUI Server data directory be located on a shared disk partition? (y/n)
==> Set to n

Do you want to change Management IP address (y/n) ?[n]> y
Enter the type of management IP address of this server (4-IPv4 / 6-IPv6) [4]> 6
Enter the management IPv6 address of this server [fc00::10:205:1:95]>
==> Management IP set to fc00::10:205:1:95

Enter the https port for NBI service [8443]>

Enter the one-time password for this Gui Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

==> CFM password set for 'cfmuser'

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the type of management IP address for primary HA server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the primary HA Server [10.205.1.95]> fc00::10:205:1:95

```

```
Enter the type of management IP address for secondary server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the secondary HA Server [10.205.1.96]> fc00::10:205:1:96

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Shared password is already set.
==> Set to

Enter number of Heartbeat links between the primary and secondary machines [1]>
==> Set to 1

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the type of machine's primary heartbeat link IP (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address for this machine's primary heartbeat link [10.205.1.95]>
fc00::10:205:1:95

Enter the type of machine's peer's primary heartbeat link IP (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the peer's primary heartbeat link [10.205.1.96]>
fc00::10:205:1:96

Enter the type of IP address for remote HA replications (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address that will be used for remote HA replications [10.205.1.96]>
fc00::10:205:1:96

Enter the port used for heartbeat communication [7802]>
==> Set to 7802

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>
==> Set to 15

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>
==> Set to 4

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter the type of IP address outside the HA cluster (4-IPv4 / 6-IPv6) [4]> 6
Enter an IP address outside of the cluster [10.205.255.254]> fc00::10:205:255:254

Enter the rsync replication timeout [3600]>
==> Set to 3600

Enter HA/database backup directory [/var/netscreen/dbbackup]>
==> Setting HA/database backup directory to /var/netscreen/dbbackup
WARNING: Directory /var/netscreen/dbbackup already exists.
Existing backups in this directory may not be
compatible with this new software.
Please exit installation and move the contents
as they will get WIPED OUT during installation.
```

The HA/database backup server(s) requires that you have previously installed the rsync program.

Enter the full path to rsync [/usr/bin/rsync]>

==> Set to /usr/bin/rsync

The HA/database backup server(s) requires that you have previously installed the ssh program.

Enter the full path for the ssh command [/usr/bin/ssh]>

==> Set to /usr/bin/ssh

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.

Please reset the trust relationship with 'nsm' user.

Here are sample commands:

```
cd /home/nsm
```

```
su nsm
```

```
ssh-keygen -t rsa
```

```
chmod 0700 .ssh
```

```
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys
```

BACKUP SETUP DETAILS

Will this machine require local database backups? (y/n) [y]>

==> Set to y

==> Setting start hour for database backup to 02

Will daily backups need to be sent to a remote machine? (y/n) [y]>

==> Set to y

Enter the type of IP address for remote backup machine (4-IPv4 / 6-IPv6) [4]> 6

Enter the IP address of the remote backup machine [fc00::10:205:1:96]>

Enter number of database backups to keep. The default value will keep the last seven backups.

The oldest backup copy will be overwritten by the new backup copy [7]>

==> Set number of database backups to keep to 7

Enter the rsync backup timeout [3600]>

==> Set to 3600

POST-INSTALLATION OPTIONS

Start High Availability daemon processes when finished? (y/n) []> y

CONFIRMATION

About to proceed with the following actions:

- Upgrade GUI Server
- Upgrade High Availability Server
- This machine will have base license with maximum 25 devices
- Store base directory for management servers as /usr/netscreen
- All Device Families Schemas Load
- This machine participates in an HA cluster
- This server is the primary: Yes
- Use IP address fc00::10:205:1:95 for management
- Use port 8443 for NBI Service
- CFM user: cfmuser

```

- CFM Password set for 'cfmuser'
- IP address for the primary HA Server: fc00::10:205:1:95
- IP address for the secondary HA Server: fc00::10:205:1:96
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: fc00::10:205:1:95
- IP address for the peer's primary heartbeat link: fc00::10:205:1:96
- IP address for remote HA replications: fc00::10:205:1:96
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: fc00::10:205:255:254
- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: fc00::10:205:1:96
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Start High Availability daemon processes when finished: Yes

```

Are the above actions correct? (y/n)> y

Primary Dev Server Output

```

[root@nsm-b3-vm9 ~]# sh nsm2012.2R10_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
WARNING:
Please make sure the following lines are present in the /etc/sysctl.conf file.
kernel.shmmax= 402653184
The install will exit if they aren't present. Please Reboot the system before
continuing
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if selinux is enabled.....ok
Checking if installed Device Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

```

```

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####

1) Upgrade Device Server from 2012.1R10 to 2012.2R10, install GUI Server
2) Clean install of Device Server, install GUI Server
3) Upgrade Device Server only from 2012.1R10 to 2012.2R10
4) Clean install of Device Server only
Enter selection (1-4) [3]>

WARNING:
You are about to upgrade the server on this machine. If you need to
backup your data before continuing, abort upgrade, backup your existing
data, and then rerun this upgrade.
Please see http://kb.juniper.net/KB3603 for details.

Hit Ctrl-C to abort upgrade or ENTER to continue

Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

Do you want to restore PostgreSQL database?(y/n) [y]> n
Select Device Schema to be loaded in NSM

1) Load all Device Family Schemas
2) Load Screen OS Device Schema only (Screen OS)
3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
Enter selection (1-3)[1]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [y]>
==> Set to y

Is this machine the primary server for the HA cluster? (y/n) [y]>
==> Set to y
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### DEVICE SERVER SETUP DETAILS #####

Will the Device Server data directory be located on a shared disk partition? (y/n)
==> Set to n

Current GUI Server IP Address is 10.205.1.95. Do you want to change the IP
(y/n)[n]> y
To enable the Device Server to communicate with the GUI Server, you must
provide the IP address of the running GUI Server
Enter the type of IP address of the running GUI Server (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address of the running GUI Server [10.205.1.95]> fc00::10:205:1:95

Do you want to change Management IP address (y/n) ?[n]> y
Enter the type of management IP address of this server (4-IPv4 / 6-IPv6) [4]> 6
Enter the management IPv6 address of this server [fc00::10:205:1:97]>
==> Management IP set to fc00::10:205:1:97

```

```
Enter the https port for NBI service [8443]>

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the type of management IP address for primary HA server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the primary HA Server [10.205.1.97]> fc00::10:205:1:97

Enter the type of management IP address for secondary server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the secondary HA Server [10.205.1.98]> fc00::10:205:1:98

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Shared password is already set.
==> Set to

Enter number of Heartbeat links between the primary and secondary machines [1]>
==> Set to 1

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the type of machine's primary heartbeat link IP (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address for this machine's primary heartbeat link [10.205.1.97]>
fc00::10:205:1:97

Enter the type of machine's peer's primary heartbeat link IP (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the peer's primary heartbeat link [10.205.1.98]>
fc00::10:205:1:98

Enter the type of IP address for remote HA replications (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address that will be used for remote HA replications [10.205.1.98]>
fc00::10:205:1:98

Enter the port used for heartbeat communication [7802]>
==> Set to 7802

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>
==> Set to 15

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>
==> Set to 4

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter the type of IP address outside the HA cluster (4-IPv4 / 6-IPv6) [4]> 6
Enter an IP address outside of the cluster [10.205.255.254]> fc00::10:205:255:254

Enter the rsync replication timeout [3600]>
==> Set to 3600
```

```

Enter HA/database backup directory [/var/netscreen/dbbackup]>
==> Setting HA/database backup directory to /var/netscreen/dbbackup
WARNING: Directory /var/netscreen/dbbackup already exists.
Existing backups in this directory may not be
compatible with this new software.
Please exit installation and move the contents
as they will get WIPED OUT during installation.

The HA/database backup server(s) requires that you have previously installed the
rsync program.
Enter the full path to rsync [/usr/bin/rsync]>
==> Set to /usr/bin/rsync

The HA/database backup server(s) requires that you have previously installed the
ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>
==> Set to /usr/bin/ssh

Note: A trust relationship between the primary and the
secondary server, via ssh-keygen, is a requirement for the
remote replication to work properly.
Please reset the trust relationship with 'nsm' user.
Here are sample commands:
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>
==> Set to y

==> Setting start hour for database backup to 02

Will daily backups need to be sent to a remote machine? (y/n) [y]>
==> Set to y

Enter the type of IP address for remote backup machine (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address of the remote backup machine [fc00::10:205:1:98]>

Enter number of database backups to keep. The default value will keep the last
seven backups.
The oldest backup copy will be overwritten by the new backup copy [7]>
==> Set number of database backups to keep to 7

Enter the rsync backup timeout [3600]>
==> Set to 3600

##### DEVSVR DB SETUP DETAILS #####

==> Postgres DevSvr Db port set to 5432

==> Postgres DevSvr Db super user set to 'nsm'

==> Postgres DevSvr Db password set for 'nsm'

```

```

##### POST-INSTALLATION OPTIONS #####

Start High Availability daemon processes when finished? (y/n) []> y

##### CONFIRMATION #####

About to proceed with the following actions:
- Upgrade Device Server
- Upgrade High Availability Server
- Store base directory for management servers as /usr/netscreen
- Restore PostgreSQL Database : No
- All Device Families Schemas Load
- This machine participates in an HA cluster
- This server is the primary: Yes
- Connect to GUI Server at fc00::10:205:1:95:7801
- Connect to GUI Server at fc00::10:205:1:95:7801
- Use IP address fc00::10:205:1:97 for management
- Use port 8443 for NBI Service
- IP address for the primary HA Server: fc00::10:205:1:97
- IP address for the secondary HA Server: fc00::10:205:1:98
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: fc00::10:205:1:97
- IP address for the peer's primary heartbeat link: fc00::10:205:1:98
- IP address for remote HA replications: fc00::10:205:1:98
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: fc00::10:205:255:254
- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: fc00::10:205:1:98
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start High Availability daemon processes when finished: Yes

Are the above actions correct? (y/n)> y

```

Upgrading NSM with HA Enabled

The process for upgrading NSM with HA enabled is as follows:

1. Perform the prerequisites steps as described in [“Prerequisite Steps” on page 19](#).
Perform the additional prerequisite steps as described in [“Introduction” on page 3](#).
2. Stop the primary and secondary GUI and Device Servers.
3. Run the NSM installer on the primary servers where you have currently installed the GUI and Device Servers. Specify that you want to upgrade the servers.

4. Configure the following HA parameters when prompted during the General Server Setup Details, the Device Server Setup Details, and the GUI Server Setup Details:
 - If this server will participate in an HA Cluster, enter **y** when prompted.
 - If this server is the primary server for the HA Cluster, enter **y** when prompted.
 - If the Device Server data directory is located on a shared disk partition, enter **y**. If you are not using a shared disk partition for the Device Server, enter **n**.
 - If the GUI server data directory is located on a shared disk partition, enter **y**. If you are not using a shared disk partition for the GUI server, enter **n**.
5. Configure the following HA parameters when prompted during the high availability (HA) setup details:
 - Enter the IP address for the primary HA Server.
 - Enter the IP address for the secondary HA Server.
 - Enter the number of HA replications.
 - Enter the number of heartbeat links between the primary and secondary machines.
 - Enter the IP address for this machine's primary heartbeat link.
 - Enter the IP address for the peer's primary heartbeat link.
 - Enter the port number used for heartbeat communication.
 - Enter a time interval in seconds between heartbeat messages.
 - Enter the number of missing heartbeat messages before automatic switchover occurs.
 - Enter an IP address outside the HA Cluster to monitor this server's network connection.
 - Enter the HA/database backup directory.
 - Type the full path to the rsync executable.
 - Type the full path for the ssh executable.
6. Run the NSM installer on the secondary server (if applicable). Configure parameters that are appropriate for the secondary server.

The NSM installer generates an installation ID and prompts you to enter the license key. For information about generating the license key, see [\[Unresolved xref\]](#).

You see output similar to the following example after generating the installation ID.

```
##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
```

```

Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if installed Device Server is newer.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers
##### EXTRACTING PAYLOADS #####
Extracting payload.....ok
Decompressing payload.....ok
Extracting license manager package.....ok
##### GATHERING INFORMATION #####
Checking device count.....ok
1) Clean install of both Device Server and GUI Server
2) Refresh both Device Server and GUI Server
Enter selection (1-2) [2]> 2
Do you want to do NSM installation with base license? (y/n) [y]> n
Will server(s) need to be reconfigured during the refresh? (y/n) [n]>
The installation ID for this system is: 2000032C62E52
Number of Devices managed by NSM is: 25
Enter the License File Path>
Removing staging directory.....ok

```



NOTE: If the NSM installer prompts you for the license file and the license key is not available, press Ctrl+Z to exit the NSM installer.

7. Enter the license key in the primary server. The NSM installer validates the license key file and stores it on the NSM Server.
8. Start the primary and secondary GUI and Device Servers.
9. Upgrade the UI client on the computers where you have installed the UI client. See [“Upgrading the User Interface” on page 170](#) for details.
10. Launch the UI and verify that you can connect to the upgraded GUI server.
11. Configure the HA cluster. See [“High Availability Overview” on page 79](#) for more information.

Typical Output with HA Enabled for IPv6 Management address

```

[root@nsm-b3-vm7 ~]# sh nsm2012.2R10_servers_linux_x86.sh

##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok

```

```

Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
WARNING:
Please make sure the following lines are present in the /etc/sysctl.conf file.
kernel.shmmax= 402653184
The install will exit if they aren't present. Please Reboot the system before
continuing
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if selinux is enabled.....ok
Checking if installed Device Server is newer.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
Checking device count.....ok

1) Clean install of both Device Server and GUI Server
2) Upgrade both Device Server and GUI Server from 2010.3r2 to 2012.2R10
Enter selection (1-2) [2]>

WARNING:
You are about to upgrade the server on this machine. If you need to
backup your data before continuing, abort upgrade, backup your existing
data, and then rerun this upgrade.
Please see http://kb.juniper.net/KB3603 for details.

Hit Ctrl-C to abort upgrade or ENTER to continue

WARNING:
NSM release 2012.2R10 requires a license to manage the devices.
License can be generated by going to www.juniper.net/customers/support and select
Contracts & Licensing
in the Support section or by contacting Juniper Customer Service.
Please obtain a license before proceeding.

Hit Ctrl-C to abort installation or ENTER to continue

The installation ID for this system is: 30002CA4ED07C

Number of Devices managed by NSM is: 573

```

```

Enter the License File Path> /root/123456789.txt
Validating License File.....ok
Enter base directory location for management servers [/usr/netscreen]>

Enable FIPS Support? (y/n) [n]>

Do you want to restore PostgreSQL database?(y/n) [y]> n
Select Device Schema to be loaded in NSM

  1) Load all Device Family Schemas
  2) Load Screen OS Device Schema only (Screen OS)
  3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
Enter selection (1-3)[1]>

##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [y]>
==> Set to y

Is this machine the primary server for the HA cluster? (y/n) [y]>
==> Set to y
WARNING: The servers need to be stopped on the secondary server
during the installation of this software to avoid data corruption.

##### DEVICE SERVER SETUP DETAILS #####

Will the Device Server data directory be located on a shared disk partition? (y/n)
==> Set to n

##### GUI SERVER SETUP DETAILS #####

Will the GUI Server data directory be located on a shared disk partition? (y/n)
==> Set to n

Do you want to change Management IP address (y/n) ?[n]> y
Enter the type of management IP address of this server (4-IPv4 / 6-IPv6) [4]> 6
Enter the management IPv6 address of this server [fc00::10:205:1:95]>
==> Management IP set to fc00::10:205:1:95

Enter the https port for NBI service [8443]>

Enter the one-time password for this Gui Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>

==> CFM user is set to 'cfmuser'

==> CFM password set for 'cfmuser'

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Enter the type of management IP address for primary HA server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the primary HA Server [10.205.1.95]> fc00::10:205:1:95

```

```

Enter the type of management IP address for secondary server (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the secondary HA Server [10.205.1.97]> fc00::10:205:1:97

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
      secondary machines.
Shared password is already set.
==> Set to

Enter number of Heartbeat links between the primary and secondary machines [1]>
==> Set to 1

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
      The IP addresses entered here must be correct and match on both ends of
      the link for automatic failover to function correctly.
Enter the type of machine's primary heartbeat link IP (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address for this machine's primary heartbeat link [10.205.1.95]>
fc00::10:205:1:95

Enter the type of machine's peer's primary heartbeat link IP (4-IPv4 / 6-IPv6)
[4]> 6
Enter the IP address for the peer's primary heartbeat link [10.205.1.97]>
fc00::10:205:1:97

Enter the type of IP address for remote HA replications (4-IPv4 / 6-IPv6) [4]> 6
Enter the IP address that will be used for remote HA replications [10.205.1.97]>
fc00::10:205:1:97

Enter the port used for heartbeat communication [7802]>
==> Set to 7802

Minimum HA failover time is 60 seconds.
The heartbeat message interval times the number of missing heartbeats
must equal at least this value.
Using the defaults is recommended.
Enter a time interval (seconds) between heartbeat messages [15]>
==> Set to 15

Enter number of missing heartbeat messages before automatic switchover occurs
[4]>
==> Set to 4

An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter the type of IP address outside the HA cluster (4-IPv4 / 6-IPv6) [4]> 6
Enter an IP address outside of the cluster [10.205.255.254]> fc00::10:205:255:254

Enter the rsync replication timeout [3600]>
==> Set to 3600

Enter HA/database backup directory [/var/netscreen/dbbackup]>
==> Setting HA/database backup directory to /var/netscreen/dbbackup
WARNING: Directory /var/netscreen/dbbackup already exists.
Existing backups in this directory may not be
compatible with this new software.
Please exit installation and move the contents
as they will get WIPED OUT during installation.

```

The HA/database backup server(s) requires that you have previously installed the rsync program.

Enter the full path to rsync [/usr/bin/rsync]>

==> Set to /usr/bin/rsync

The HA/database backup server(s) requires that you have previously installed the ssh program.

Enter the full path for the ssh command [/usr/bin/ssh]>

==> Set to /usr/bin/ssh

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.

Please reset the trust relationship with 'nsm' user.

Here are sample commands:

```
cd /home/nsm
```

```
su nsm
```

```
ssh-keygen -t rsa
```

```
chmod 0700 .ssh
```

```
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys
```

BACKUP SETUP DETAILS

Will this machine require local database backups? (y/n) [y]>

==> Set to y

==> Setting start hour for database backup to 02

Will daily backups need to be sent to a remote machine? (y/n) [y]>

==> Set to y

Enter the type of IP address for remote backup machine (4-IPv4 / 6-IPv6) [4]> 6

Enter the IP address of the remote backup machine [fc00::10:205:1:97]>

Enter number of database backups to keep. The default value will keep the last seven backups.

The oldest backup copy will be overwritten by the new backup copy [7]>

==> Set number of database backups to keep to 7

Enter the rsync backup timeout [3600]>

==> Set to 3600

DEVSVR DB SETUP DETAILS

==> Postgres DevSvr Db port set to 5432

==> Postgres DevSvr Db super user set to 'nsm'

==> Postgres DevSvr Db password set for 'nsm'

POST-INSTALLATION OPTIONS

Start High Availability daemon processes when finished? (y/n) [y]> y

CONFIRMATION

About to proceed with the following actions:

- Upgrade Device Server

```

- Upgrade GUI Server
- Upgrade High Availability Server
- Store base directory for management servers as /usr/netscreen
- Restore PostgreSQL Database : No
- All Device Families Schemas Load
- This machine participates in an HA cluster
- This server is the primary: Yes
- Use IP address fc00::10:205:1:95 for management
- Use port 8443 for NBI Service
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- IP address for the primary HA Server: fc00::10:205:1:95
- IP address for the secondary HA Server: fc00::10:205:1:97
- Set shared password for heartbeat
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: fc00::10:205:1:95
- IP address for the peer's primary heartbeat link: fc00::10:205:1:97
- IP address for remote HA replications: fc00::10:205:1:97
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: fc00::10:205:255:254
- Become primary in the event of a tie: y
- HA rsync command replication timeout: 3600
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: fc00::10:205:1:97
- Number of database backups to keep: 7
- HA rsync command backup timeout: 3600
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start High Availability daemon processes when finished: Yes

Are the above actions correct? (y/n)> y

```

Upgrading the Database Backup Files

If your previous installation of NSM included high availability, you will also need to upgrade the data in your previous local and remote database backup directories. We recommend that you do so manually by running the `replicateDb` script on the primary server. See [“Backing Up the Database Locally” on page 262](#) for more information. If you do not manually replicate the database, the upgrade occurs automatically during the next scheduled remote database replication interval (default is 1 hour).

If the primary server goes down before the next scheduled remote database replication, the data on the secondary server will not be upgraded. You will need to perform a manual data replication/upgrade on the secondary server.

Restoring Data if the Upgrade Fails

If the upgrade fails, you can restore data from your previous installation. This is only possible if you performed the required backup of your GUI server configuration data and Device Server log data before performing the upgrade and migration process.

The process for restoring your previous installation is as follows:

1. Remove all existing components of the NSM management system. See [“Removing the Management System” on page 270](#) for more information.
2. Perform a clean installation of NSM. Refer to the appropriate version of NSM documentation for more information about installing your version of NSM.
3. Restore your configuration and log data from backup. See [“Archiving and Restoring Logs and Configuration Data” on page 258](#) for more information.

Next Steps

Now that you have completed installing the NSM management system with HA enabled, you are ready to begin managing your network. Refer to the *Network and Security Manager Administration Guide* and *Network and Security Manager Online Help* for information describing how to plan and implement NSM for your network.

CHAPTER 6

Upgrading NSM Appliances to NSM 2012.2

This chapter describes how to upgrade the management system on NSMXpress and NSM3000 Regional Servers, and NSM Central Manager (NSM CM) to Network and Security Manager (NSM) 2012.2. This chapter also describes how to migrate your database from a Linux or Solaris server to an NSM appliance, and provides instructions for changing user privileges in the NSM appliance.

This chapter contains the following sections:

- [Prerequisite Steps on page 189](#)
- [Upgrading an NSM Appliance in a Standalone Setup on page 190](#)
- [Upgrading NSM Regional Server and NSM CM Appliances Using Specific Files on page 196](#)
- [Upgrading an NSM Appliance in an HA Setup on page 208](#)
- [Upgrading an NSM Appliance in an Extended HA Setup on page 218](#)
- [Migrating Data to an NSM Regional Server Appliance on page 225](#)
- [User Privileges on an NSM Appliance on page 230](#)

Prerequisite Steps

Before you upgrade the management system, you need to perform the following prerequisite steps:

1. Take a backup of the NSM configuration. For details see <https://kb.juniper.net/KB11476>.
2. Using your current version of NSM, upgrade any devices running ScreenOS 4.0.x or earlier version or remove them from your managed network. ScreenOS devices must run ScreenOS 5.0 or later version to be managed by NSM 2008.1 or later release. The NSM installer stops with errors if ScreenOS 4.0.x devices are present in the NSM database.
3. Ensure that the NSM appliance is accessible through a serial console.
4. Log in to the appliance as root. If you have logged in as admin user in NSM appliance, enter **sudo su -** and the admin password to gain root access.



NOTE: Although the management system runs with nsm user permissions, you must have root permissions to run the NSM installer.

5. Check for sufficient free disk space. For this, run the **df -h** command. Make sure that **/tmp** has only 50 MB-200 MB used space (not more than 200 MB used space). If sufficient free space is not available, delete the large files and directories. To find the large files hidden under the directory, run the **# du | sort -rn | head -n 10** command.

See “[Hardware Recommendations](#)” on [page 283](#) for more information about the disk space requirements appropriate for your specific network.

6. If you plan to manage more than 25 devices, you must obtain a license key file from the Juniper License Management Server (LMS) and install that file on the NSM Server or the NSM appliance. See [\[Unresolved xref\]](#).
7. Increase the rsync backup timeout and rsync replication timeout values to 3600. See “[Setting the rsync Timeout Values](#)” on [page 156](#).
8. To check the kernel name and current OS version of NSM appliance, use the command **# uname -r**.

If the command output is **2.6.18-274.el5PAE**, then the appliance OS version is CentOS5.7.

If the command output is **2.6.9-67.0.20.ELsmp**, then the appliance OS version is CentOS 4.X.

Upgrading an NSM Appliance in a Standalone Setup

This topic describes how to upgrade an NSM appliance in a standalone setup.

1. Perform the steps as described in “[Prerequisite Steps](#)” on [page 189](#).

In NSM Release 2012.2R1 and later releases, a generic ZIP file is available for upgrades.

The generic ZIP file is a system package that contains the latest updated packages that are required for upgrading the NSM appliance version.

A separate downloadable ZIP package for appliances is not used for service releases. Use the latest Generic Upgrade package from the [Software download site](#). The NSM installer now has the capability to modify the version information on NSM appliances.

The files required for the offline upgrade of the NSM appliance to the NSM 2012.2 service release are listed in [Table 20 on page 191](#). The files can be downloaded from <http://www.juniper.net/customers/csc/software/>.

Table 20: Files for Offline Upgrade

Filename	Download Link
nsm_generic_offline_upgrade_CentOS4.x.zip	NSM Appliance Generic Offline Upgrade Package_vX-CentOS 4.x (X in vX represents the latest version of the generic ZIP file/generic online upgrade script.)
nsm_generic_offline_upgrade_CentOS5.x.zip	NSM Appliance Generic Offline Upgrade Package_vX-CentOS 5.x (X in vX represents the latest version of the generic ZIP file/generic online upgrade script.)
nsm2012.2RX_servers_linux_x86.zip	Linux Server (for NSM Regional Server)
nsm2012.2RX_servers_upgrade_cm.zip	Central Manager (for NSM Central Manager)

**NOTE:**

- If you have already upgraded the NSM appliance to NSM version 2012.2 and want to upgrade to any release between 2012.2R1 and 2012.2R4, you can upgrade using just the Linux build of the respective service release. However, to upgrade to service releases 2012.2R5 or later, from 2012.2, use version 2 of the generic offline or online files in addition to with the Linux build.
- If you have chosen online mode, you need to copy only the `upgrade-os.sh` file from the NSM Appliance Generic Online Upgrade Script_vX (X represents the version of the generic online upgrade script) link on the [Juniper Networks Software Download site](#) along with the desired 2012.2 Linux build to the NSM appliance.

2. Copy the following files to your NSM appliance using FTP or SCP:
 - `nsm_generic_offline_upgrade_CentOS4.x.zip`: Offline mode for CentOS 4.X.
 - `nsm_generic_offline_upgrade_CentOS5.x.zip`: Offline mode for CentOS 5.7.
 - `nsm2012.2RX_servers_linux_x86.zip` (X in 2012.2RX represents the required version of the Linux Server Installer for NSM).
3. Unzip the required file using the `unzip` `<Name_of_the_generic_offline_upgrade_on_OS_version.zip>` command, on the NSM appliance. Example: `unzip nsm_generic_offline_upgrade_CentOS5.x.zip`
4. Extract the latest NSM 2012.2 service release Linux build using the `unzip` `<Name_of_the_Linux_build_of_service_Release.zip>` command, on the NSM appliance. Example: `unzip nsm2012.2R2_servers_linux_x86.zip`

5. To start the upgrade, run the **sh upgrade-os.sh**
<Name_of_the_Linux_build_of_service_Release.sh> **Offline/Online** command on the server.

Example: To perform an offline upgrade to NSM 2012.2R2, use the **sh upgrade-os.sh nsm2012.2R2_servers_linux_x86.sh Offline** command.

To perform an online upgrade to NSM2012.2R2, run the **sh upgrade-os.sh nsm2012.2R2_servers_linux_x86.sh Online** command.

The **upgrade-os.sh** script prompts you to back up the NSM Profiler DB. Later, the NSM installer uses the NSM Profiler DB backup to restore the data.



NOTE: The **upgrade-os.sh** file prompts you for the NSM Profiler DB backup only if the NSM appliance is running CentOS 5.7.

The **upgrade-os.sh** script updates the system packages and runs the NSM installer. The NSM installer begins a series of pre-installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You have correctly logged in as root user.
- You have installed a version of NSM earlier than the current version you are installing.
- The system has sufficient disk space and RAM.



NOTE:

- **Done** indicates that the NSM installer successfully performed a task.
- **OK** indicates that the NSM installer performed a check and verified that the condition was satisfied.
- **FAILED** indicates that the NSM installer performed a task or check, but it was not successful. See the install log for information about the failure.



NOTE: Logs are usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of installation, the log might be in `/tmp`.

6. Type **2** to specify that you want to upgrade GUI server and Device server.



NOTE:

- The NSM installer displays the **Refresh** option if the currently installed version and the version being installed are same. For example, if you install NSM 2012.2R5 on NSM 2012.2R5, the NSM installer displays the **Refresh** option.
- For upgrades to major release versions, the NSM installer displays the **Upgrade** option instead of the **Refresh** option. For example, if you upgrade from NSM 2010.3 to NSM 2012.2, the NSM installer displays the **Upgrade** option.
- For upgrades to minor release versions, the NSM installer displays the **Patch** option instead of the **Refresh** option. For example, if you upgrade from NSM 2012.2R1 to NSM 2012.2R5, the NSM installer displays the **Patch** option.

7. The NSM installer conducts checks for license requirement and if required, it prompts you to enter the license key file. When you enter the license key file, the NSM installer validates the license key file and stores it on the NSM server.

- The NSM installer checks the number of devices managed by the NSM, and if there are more than 25 devices, it displays a warning message about the license requirement. After you press Enter to proceed, the NSM installer displays the installation ID and the number of devices. If a license key is already available, the installer validates the existing license key. If a license key is not available, the installer prompts for the location of the license file.
- If there are 25 or fewer devices in NSM and no license exists, the installer prompts you to use the base license.

If you enter **y** (yes), the NSM installer proceeds with the NSM upgrade. If you enter **n** (no), it displays the installation ID and number of devices in NSM and prompts you for the location of the license file.

However, if a license was already installed, the NSM installer validates it and continues with the installation.



NOTE: If the NSM installer prompts you for the license file and the license key is not available, press **Ctrl+Z** to exit the NSM installer.

For information about generating the license key, see [\[Unresolved xref\]](#).

The NSM installer script output is as follows:

```
##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
```

```

Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if installed Device Server is newer.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
Checking device count.....ok

1) Clean install of both Device Server and GUI Server
2) Upgrade both Device Server and GUI Server from 2011.4 to 2012.2R4
Enter selection (1-2) [2]> 2

WARNING:
You are about to upgrade the server on this machine. If you need to
backup your data before continuing, abort upgrade, backup your existing
data, and then rerun this upgrade.
Please see http://kb.juniper.net/KB3603 for details.

Hit Ctrl-C to abort upgrade or ENTER to continue

Do you want to do NSM installation with base license? (y/n) [y]> n

The installation ID for this system is: 0213032010200006

Number of Devices managed by NSM is: 0

Enter the License File Path>

```

8. On the NSM appliance, the NSM installer prompts you to restore the NSM Profiler DB.

Do you want to restore PostgreSQL database?(y/n) [y]>



NOTE: Enter n if the NSM appliance is running on CentOS4.x.

When you type **y** or press Enter, the restore procedure prompts you for the file path of the NSM Profiler DB backup.

Enter PostgreSQL data backup file location [/var/netscreen/DevSvr]

9. The NSM installer prompts you to select the device schemas that need to be installed. Depending on the device models being managed by NSM, select the appropriate option. By default, all device schemas are selected.



NOTE: The NSM installer does not prompt for the step 10 if you are patching from NSM 2012.2 to 2012.2Rx.

10. If you are upgrading NSM to a 2012.2 service release from a version earlier than 2012.2, the NSM installer prompts you for a one-time password for the GUI server.

Enter the one-time password for this Gui Server

Enter password (password will not display as you type) >

Please enter again for verification

Enter password (password will not display as you type) >

11. The NSM installer prompts you to restart the services when the upgrade is complete. Type **y** and press Enter to restart the servers when finished.

12. The NSM installer prompts you to verify your upgrade configuration settings. If the configuration settings are correct, type **y** and press Enter to proceed. If the configuration settings are incorrect, type **n** and press Enter to return to the original selection prompt.

The upgrade proceeds automatically. The NSM installer performs the following actions:

- Upgrades the Device server
- Upgrades the GUI server
- Upgrades the HA server
- Sets startup scripts

13. The NSM installer performs post-installation tasks such as removing the staging directory and starting the server processes (if configured).

The installation script logs the actions that it performs, to help in troubleshooting. At the end of the upgrade process, the NSM installer saves the log file in **/usr/netscreen/DevSvr/var/errorLog/** and provides the name of the installation log file.

14. After the successful installation, move the NSM Linux installer file to `/var/install` (example: `mv nsm2012.2R2_servers_linux_x86.sh /var/install`), and enter the following commands under `/var/install`:

- `rm -f NSM-RS`
- `ln -s <Name_of_the_Linux_build_of_service_Release.sh> NSM-RS`
- `chmod 755 NSM-RS`



NOTE: For NSM-CM appliances, enter the following commands:

- `rm -f NSM-CM`
- `ln -s <Name_of_the_CM_build_of_service_Release.sh> NSM-CM`
- `chmod 755 NSM-CM`

15. Start the NSM services.
16. Upgrade the GUI client on the computers where you have installed the UI client. See [“Upgrading the User Interface” on page 170](#) for details.
17. Launch the GUI and verify that you can connect to the upgraded GUI server.

Upgrading NSM Regional Server and NSM CM Appliances Using Specific Files

Upgrading to NSM Release 2012.2 on an NSM Regional Server Appliance (Online mode)

This section describes how to upgrade to NSM 2012.2 on an NSM Regional Server appliance if the appliance is connected to the Internet.

NSM 2012.2 requires a license file if you are managing more than 25 devices. You must have the license file before performing the upgrade to NSM 2012.2. The NSM installer will not proceed without the license file.

For information on the procedure for generating the license file, refer to [\[Unresolved xref\]](#).

Use the following procedure to upgrade to NSM 2012.2 on an NSMXpress or an NSM3000 Regional Server appliance.

1. From the [NSM Software Download](#) page, click the **NSM Appliance Upgrade CentOS 4.x Regional Server** or **NSM Appliance Upgrade CentOS 5.7 Regional Server** link to download the appropriate NSM appliance software.
2. Copy and save the required files (for example:
`CentOS4.x_nsm2012.2_servers_upgrade_RS.tar.bz2` for CentOS 4.x, or

CentOS5.7_nsm2012.2_servers_upgrade_RS.tar.bz2 for CentOS 5.7) to your NSM appliance under **/var/** subdirectory using FTP or SCP.

3. Log in as the admin user, and enter **n** when prompted to run the setup wizard.
4. Enter **sudo su -** and the admin password to gain root access.
5. Navigate to the **/var/** subdirectory and extract the downloaded file using the command **tar -jxvf zipfile.tar.bz2**.

Example:

- **tar -jxvf CentOS5.7_nsm2012.2_servers_upgrade_RS.tar.bz2**
- **tar -jxvf CentOS4.x_nsm2012.2_servers_upgrade_RS.tar.bz2**

The extracted file contains the following files: **nsm2012.2_servers_upgrade_rs.zip** and **nsm2012.2_offline_upgrade.zip**

6. Confirm that the **unzip** utility is present on the NSM appliance by entering the following command:

```
which unzip
```

This command returns the location of the **unzip** utility. If it is not available, use the following command to install this utility:

```
yum install unzip
```

7. Enter the following command to unzip the **nsm2012.2_servers_upgrade_rs.zip** file on the NSM appliance:

```
unzip nsm2012.2_servers_upgrade_rs.zip
```

8. Enter the following command to automatically start the installation:

```
sh upgrade-os.sh nsm2012.2_servers_linux_x86.sh
```

The NSM installer begins a series of pre installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You correctly logged in as root.
- You have installed a version of NSM earlier than the current version you are installing.
- The system has sufficient disk space and RAM.



NOTE: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the NSM installer successfully performed a task.
- “OK” indicates that the NSM installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the NSM installer performed a task or check, but it was not successful. See the install log for information about the failure. This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of installation, the log might be in `/var/tmp`.

The NSM installer then stops any running servers.

9. Type **2** to specify that you want to upgrade both the Device Server and the GUI server.



NOTE: If you specify that you want to upgrade the Device Server and GUI server, all data previously configured in the system is restored. If you do not want to restore your previous configuration data, choose to have the NSM installer perform a clean install of NSM.

10. The NSM installer next prompts you to configure additional options specific to your installation during the upgrade. These options can include:

- Configuring High Availability
- Configuring interoperability with NetScreen-Statistical Report Server
- Configuring backup options
- Configuring the client download and NBI port

If applicable, follow the NSM installer prompts to configure these options.

The NSM installer next prompts you to restart the servers when the installation is finished.

11. Type **y** and press **Enter** to restart the servers when finished. Type **n** and press **Enter**, if you do not want to restart server processes.

The NSM installer prompts you to verify your upgrade configuration settings.

12. Verify your settings. If are correct, type **y** and press **Enter** to proceed. If the configuration settings are incorrect, type **n** and press **Enter** to the previous prompt.

The upgrade proceeds automatically. The NSM installer performs the following actions:

- Extracts and decompresses the software payloads.
- Upgrades the Device server.
- Upgrades the GUI server.
- Installs the HA server.
- Sets start scripts.
- Performs post installation tasks such as removing the staging directory and starting the server processes (if configured).

Messages display the installation progress.

After the installation finishes, it generates a log file with the output of the installation commands for troubleshooting. The NSM installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `/usr/netscreen/DevSvr/var/errorLog` subdirectory.

13. After the successful installation, copy the NSM installer file `nsm2012.2_servers_linux_x86.sh` to the `/var/install` directory and enter the following commands:

```
rm -f NSM-RS
chmod 755 nsm2012.2_servers_linux_x86.sh
ln -s nsm2012.2_servers_linux_x86.sh NSM-RS
```

Upgrading to NSM 2012.2 Release on an NSM Central Manager Appliance (Online mode)

This section describes how to upgrade to NSM 2012.2 on an NSM Central Manager appliance if the appliance is connected to the Internet.



NOTE: NSM 2012.2 for Central Manager does not require a license file.

Use the following procedure to upgrade to NSM 2012.2 on an NSM CM appliance.

1. From the [NSM Software Download](#) page, click the **NSM Appliance Upgrade CentOS 4.x Central Manager** or **NSM Appliance Upgrade CentOS 5.7 Central Manager** link to download the appropriate NSM appliance software.
2. Copy and save the required file (for example: `CentOS4.x_nsm2012.2_servers_upgrade_CM.tar.bz2` for CentOS4.x, or `CentOS5.7_nsm2012.2_servers_upgrade_CM.tar.bz2` for CentOS5.7) to your NSM appliance under `/var/` subdirectory using FTP or SCP.
3. Log in as the admin user, and enter `n` when prompted to run the setup wizard.

4. Enter **sudo su -** and enter the admin password to gain root access.
5. Navigate to the **/var/** subdirectory and extract the downloaded file using the command **tar -jxvf zipfile.tar.bz2**.

Example:

- **tar -jxvf CentOS5.7_nsm2012.2_servers_upgrade_CM.tar.bz2**
- **tar -jxvf CentOS4.x_nsm2012.2_servers_upgrade_CM.tar.bz2**

The extracted file contains the following files: **nsm2012.2_servers_upgrade_cm.zip** and **nsm2012.2_offline_upgrade.zip**.

6. Confirm that the **unzip** utility is present on the NSM CM appliance by entering the following command:

```
which unzip
```

This command gives you the location of the **unzip** utility. If it is not available, use the following command to install this utility:

```
yum install unzip
```

7. Enter the following command to unzip the **nsm2012.2_servers_upgrade_cm.zip** file on the NSM Central Manager system:

```
unzip nsm2012.2_servers_upgrade_cm.zip
```

8. Enter the following command to automatically start the installation.

```
sh upgrade-os.sh nsm2012.2_servers_cm.sh
```

The NSM installer begins a series of pre installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You correctly logged in as root.
- You have installed a version of NSM earlier than the current version you are installing.
- The system has sufficient disk space and RAM.



NOTE: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the NSM installer successfully performed a task.
- “OK” indicates that the NSM installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the NSM installer performed a task or check, but it was not successful. See the install log for information about the failure. This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of installation, the log might be in `/var/tmp`.

The NSM installer then stops any running servers.

9. Type **1** to specify that you want to upgrade the Central Manager server.



NOTE: If you specify that you want to upgrade the Central Manager server, all data previously configured in the system is restored. If you do not want to restore your previous configuration data, choose to have the NSM installer perform a clean install of Central Manager.

10. The NSM installer next prompts you to configure additional options specific to your installation during the upgrade. These options can include:

- Configuring High Availability
- Configuring backup options
- Configuring the client download and NBI ports

If applicable, follow the NSM installer prompts to configure these options.

The NSM installer next prompts you to restart the servers when the installation is finished.

11. Type **y** and press Enter to restart the servers when finished. Type **n** and press Enter if you do not want to restart server processes.

The NSM installer prompts you to verify your upgrade configuration settings.

12. Verify your settings. If the configuration settings are correct, type **y** and press **Enter** to proceed. If settings are not correct, or type **n** and press **Enter** to return to the previous prompt.

The upgrade proceeds automatically. The NSM installer performs the following actions:

- Extracts and decompresses the software payloads.
- Upgrades Central Manager.
- Installs the HA Server.
- Sets start scripts.
- Performs post installation tasks such as removing the staging directory and starting the server processes (if configured).

Messages display the installation progress.

After the installation finishes, it generates a log file with the output of the installation commands for troubleshooting. The NSM installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `/usr/netscreen/GuiSvr/var/errorLog` subdirectory.

13. After successful installation, copy the NSM installer file `nsm2012.2_servers_cm.sh` to the `/var/install` directory and enter the following commands:

```
rm -f NSM-CM
chmod 755 nsm2012.2_servers_cm.sh
ln -s nsm2012.2_servers_linux_cm.sh NSM-CM
```

Upgrading to NSM 2012.2 Release on an NSM Regional Server Appliance (Offline Mode)

The section provides instructions on upgrading to NSM 2012.2 on an NSM appliance if the NSM appliance is not connected to the Internet.

1. From the [NSM Software Download](#) page, click the **NSM Appliance Upgrade CentOS 4.x Central Manager** or **NSM Appliance Upgrade CentOS 5.7 Central Manager** link to download the appropriate NSM appliance software.
2. Copy and save the required file (for example: `CentOS4.x_nsm2012.2_servers_upgrade_RS.tar.bz2` for CentOS 4.x, or `CentOS5.7_nsm2012.2_servers_upgrade_RS.tar.bz2` for CentOS 5.7) to your NSM appliance under `/var/` subdirectory using FTP or SCP.
3. Log in as the admin user, and answer `n` when prompted to run the setup wizard.
4. Enter the following command, and then enter the admin password to gain root access.

```
sudo su -
```

5. Navigate to the `/var/` subdirectory and extract the downloaded file using the command `tar -jxvf zipfile.tar.bz2`.

Example:

- `tar -jxvf CentOS5.7_nsm2012.2_servers_upgrade_RS.tar.bz2`
- `tar -jxvf CentOS4.x_nsm2012.2_servers_upgrade_RS.tar.bz2`

The extracted file contains the following files: `nsm2012.2_servers_upgrade_rs.zip` and `nsm2012.2_offline_upgrade.zip`.

6. Confirm that the **unzip** utility is present on the NSM appliance by entering the following command:

```
which unzip
```

This command returns the location of the **unzip** utility. If it is not available, the **unzip** utility is provided on the [NSM Software Download](#) page. Use the following command to install this utility:

```
rpm -i unzip-5.51-9.EL4.5.i386.rpm
```

7. Enter the following command to unzip the `nsm2012.2_servers_upgrade_rs.zip` file on the NSM appliance:

```
unzip nsm2012.2_servers_upgrade_rs.zip
```

8. Enter the following command to start the installation.

```
sh upgrade-os.sh nsm2012.2_servers_linux_x86.sh Offline
```

The NSM installer begins a series of pre installation checks that ensure:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You correctly logged in as root.
- You have installed a version of NSM earlier than the current version you are installing.
- The system has sufficient disk space and RAM.



.....

NOTE: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the NSM installer successfully performed a task.
 - “OK” indicates that the NSM installer performed a check and verified that the condition was satisfied.
 - “FAILED” indicates that the NSM installer performed a task or check, but it was not successful. See the install log for information about the failure. This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of installation, the log might be in `/var/tmp`.
-

The NSM installer then stops any running servers.

9. Type **2** to specify that you want to upgrade both the Device Server and the GUI server.



NOTE: If you specify that you want to upgrade the Device Server and the GUI server, all data previously configured in the system is restored. If you do not want to restore your previous configuration data, choose to have the NSM installer perform a clean install of NSM.

10. The NSM installer next prompts you to configure additional options specific to your installation during the upgrade. These options can include:

- Configuring high availability
- Configuring interoperability with NetScreen Statistical Report Server
- Configuring backup options
- Configuring the client download and NBI port

If applicable, follow the NSM installer prompts to configure these options.

The NSM installer next prompts you to restart the servers when the installation is finished.

11. Type **y** and press Enter to restart the servers when finished. Type **n** and press Enter if you do not want to restart server processes.

The NSM installer prompts you to verify your upgrade configuration settings.

12. Verify your settings. If the configuration settings are correct, type **y** and press **Enter** to proceed. If the configuration settings are incorrect, type **n** and press **Enter** to return to the previous prompt.

The upgrade proceeds automatically. The NSM installer performs the following actions:

- Extracts and decompresses the software payloads.
- Upgrades the Device server.
- Upgrades the GUI server.
- Installs the HA server.
- Sets start scripts.
- Performs post installation tasks such as removing the staging directory and starting the server processes (if configured).

Messages display the installation progress.

After the installation finishes, it generates a log file with the output of the installation commands for troubleshooting. The NSM installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `/usr/netscreen/DevSvr/var/errorLog` subdirectory.

13. After successful installation, copy the NSM installer file `nsm2012.2_servers_linux_x86.sh` to the `/var/install` directory and enter the following commands:

```
rm -f NSM-RS
chmod 755 nsm2012.2_servers_linux_x86.sh
ln -s nsm2012.2_servers_linux_x86.sh NSM-RS
```

Upgrading to NSM Release 2012.2 on an NSM Central Manager Appliance (Offline Mode)

This section provides instruction on upgrading to NSM 2012.2 on the NSM Central Manager appliance if the NSM Central Manager appliance is not connected to the Internet.

1. From the [NSM Software Download](#) page, click the **NSM Appliance Upgrade CentOS 4.x Central Manager** or **NSM Appliance Upgrade CentOS 5.7 Central Manager** link to download the appropriate NSM appliance software.
2. Copy and save the required file (for example, `CentOS4.x_nsm2012.2_servers_upgrade_CM.tar.bz2` for CentOS4.x, or `CentOS5.7_nsm2012.2_servers_upgrade_CM.tar.bz2` for CentOS5.7) to your NSM appliance under `/var/` subdirectory using FTP or SCP.
3. Log in as the admin user, and type `n` when prompted to run the setup wizard.
4. Enter the following command, and then enter the admin password to gain root access.

```
sudo su -
```

5. Navigate to the `/var/` subdirectory and extract the downloaded file using the command `tar -jxvf zipfile.tar.bz2`.

Example:

- `tar -jxvf CentOS5.7_nsm2012.2_servers_upgrade_CM.tar.bz2`
- `tar -jxvf CentOS4.x_nsm2012.2_servers_upgrade_CM.tar.bz2`

The extracted file contains the following files: `nsm2012.2_servers_upgrade_cm.zip` and `nsm2012.2_offline_upgrade.zip`

6. Confirm that the `unzip` utility is present on the NSM CM appliance by entering the following command:

```
which unzip
```

This command returns the location of the `unzip` utility. If it is not available, the `unzip` utility is provided on the [NSM Software Download](#) page. Use the following command to install this utility:

```
rpm -i unzip-5.51-9.EL4.5.i386.rpm
```

7. Enter the following command to unzip the **nsm2012.2_servers_upgrade_cm.zip** file on the NSM Central Manager appliance:

```
unzip nsm2012.2_servers_upgrade_cm.zip
```

8. Enter the following command to automatically start the installation:

```
sh upgrade-os.sh nsm2012.2_servers_cm.sh Offline
```

The NSM installer begins a series of pre installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You correctly logged in as root.
- You have installed a version of NSM earlier than the current version you are installing.
- The system has sufficient disk space and RAM.



NOTE: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the NSM installer successfully performed a task.
- “OK” indicates that the NSM installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the NSM installer performed a task or check, but it was not successful. See the install log for information about the failure. This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of installation, the log might be in `/var/tmp`.

The NSM installer then stops any running servers.

9. Type **1** to specify that you want to upgrade the Central Manager server.



NOTE: If you specify that you want to upgrade the Central Manager, all data previously configured in the system is restored. If you do not want to restore your previous configuration data, choose to have the NSM installer perform a clean install of the Central Manager.

10. The NSM installer next prompts you to configure additional options specific to your installation during the upgrade. These options can include:

- Configuring High Availability
- Configuring backup options
- Configuring the client download and NBI ports

If applicable, follow the NSM installer prompts to configure these options.

The NSM installer next prompts you to restart the servers when the installation is finished.

11. Type **y** and press Enter to restart the servers when finished. Type **n** and press Enter if you do not want to restart server processes.

The NSM installer prompts you to verify your upgrade configuration settings.

12. Verify your settings. If the configuration settings are correct, type **y** and press **Enter** to proceed. If the configuration settings are incorrect, type **n** and press **Enter** to return to the previous prompt.

The upgrade proceeds automatically. The NSM installer performs the following actions:

- Extracts and decompresses the software payloads.
- Upgrades the Central Manager.
- Installs the HA server.
- Sets start scripts.
- Performs post installation tasks such as removing the staging directory and starting the server processes (if configured).

Messages display the installation progress.

After the installation finishes, it generates a log file with the output of the installation commands for troubleshooting. The NSM installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `/usr/netscreen/GuiSrv/var/errorLog` subdirectory.

13. After the successful installation, copy the NSM installer file (`nsm2012.2_servers_cm.sh`) to the `/var/install` directory and then enter the following commands:

```
rm -f NSM-CM
chmod 755 nsm2012.2_servers_cm.sh
ln -s nsm2012.2_servers_linux_cm.sh NSM-CM
```

Upgrading an NSM Appliance in an HA Setup

This topic describes how to upgrade an NSM appliance in an HA setup (two separate appliances).

1. Perform the steps as described in “Prerequisite Steps” on page 189.

In NSM Release 2012.2R1 and later releases, a generic ZIP file is available for upgrades.

The generic ZIP file is a system package that contains the latest updated packages that are required for upgrading the NSM appliance version.

A separate downloadable ZIP package for appliances is not used for service releases. Use the latest Generic Upgrade package from the [Software download site](#). The NSM installer now has the capability to modify the version information on NSM appliances.

The files required for the offline upgrade of the NSM appliance to the NSM 2012.2 service release are listed in [Table 20 on page 191](#). The files can be downloaded from <http://www.juniper.net/customers/csc/software/>.

Table 21: Files for Offline Upgrade

Filename	Download Link
nsm_generic_offline_upgrade_CentOS4.x.zip	NSM Appliance Generic Offline Upgrade Package_vX-CentOS 4.x (X in vX represents the latest version of the generic ZIP file/generic online upgrade script.)
nsm_generic_offline_upgrade_CentOS5.x.zip	NSM Appliance Generic Offline Upgrade Package_vX-CentOS 5.x (X in vX represents the latest version of the generic ZIP file/generic online upgrade script.)
nsm2012.2RX_servers_linux_x86.zip	Linux Server (for NSM Regional Server)
nsm2012.2RX_servers_upgrade_cm.zip	Central Manager (for NSM Central Manager)

**NOTE:**

- If you have already upgraded the NSM appliance to NSM version 2012.2 and want to upgrade to any release between 2012.2R1 and 2012.2R4, you can upgrade using just the Linux build of the respective service release. However, to upgrade to service releases 2012.2R5 or later, from 2012.2, use version 2 of the generic offline or online files in addition to with the Linux build.
- If you have chosen online mode, you need to copy only the `upgrade-os.sh` file from the NSM Appliance Generic Online Upgrade Script_vX (X represents the version of the generic online upgrade script) link on the [Juniper Networks Software Download site](#) along with the desired 2012.2 Linux build to the NSM appliance.

2. Copy the following files to your NSM appliance using FTP or SCP:
 - `nsm_generic_offline_upgrade_CentOS4.x.zip`: Offline mode for CentOS 4.X.
 - `nsm_generic_offline_upgrade_CentOS5.x.zip`: Offline mode for CentOS 5.7.
 - `nsm2012.2RX_servers_linux_x86.zip` (X in 2012.2RX represents the required version of the Linux Server Installer for NSM).
3. Unzip the required file using the `unzip` `<Name_of_the_generic_offline_upgrade_on_OS_version.zip>` command, on the NSM appliance. Example: `unzip nsm_generic_offline_upgrade_CentOS5.x.zip`
4. Extract the latest NSM 2012.2 service release Linux build using the `unzip` `<Name_of_the_Linux_build_of_service_Release.zip>` command, on the NSM appliance. Example: `unzip nsm2012.2R2_servers_linux_x86.zip`

5. First, stop the HA server service on the appliance that is in the standby state, and then stop the HA server service on the appliance that is in the active state. Use the `/usr/netscreen/HaSvr/utls/haStatus` command to identify the state of the appliances. Ensure that they are in sync.

To stop HA servers, use the following command:

```
# /etc/init.d/haSvr stop
```

6. Identify the appliance that is configured as the primary server and the appliance that is configured as the secondary server by checking the IP addresses configured for the `highAvail.primaryServerIp` and `highAvail.secondaryServerIp` parameters in `/usr/netscreen/HaSvr/var/haSvr.cfg`.

7. To start the upgrade, run the `sh upgrade-os.sh` `<Name_of_the_Linux_build_of_service_Release.sh> Offline/Online` command on the primary server (identified in step 6) and then run the command on the secondary server.

Example: To perform an offline upgrade to NSM 2012.2R2, use the `sh upgrade-os.sh nsm2012.2R2_servers_linux_x86.sh Offline` command.

To perform an online upgrade to NSM 2012.2R2, run the `sh upgrade-os.sh nsm2012.2R2_servers_linux_x86.sh Online` command.

The `upgrade-os.sh` script prompts you to back up the NSM Profiler DB. Later, the NSM installer uses the NSM Profiler DB backup to restore the data.



NOTE: The `upgrade-os.sh` file prompts you for the NSM Profiler DB backup only if the NSM appliance is running CentOS 5.7.

The `upgrade-os.sh` script updates the system packages and runs the NSM installer. The NSM installer begins a series of pre-installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You have correctly logged in as root user.
- You have installed a version of NSM earlier than the current version you are installing.
- The system has sufficient disk space and RAM.

**NOTE:**

- Done indicates that the NSM installer successfully performed a task.
- OK indicates that the NSM installer performed a check and verified that the condition was satisfied.
- FAILED indicates that the NSM installer performed a task or check, but it was not successful. See the install log for information about the failure.



NOTE: Logs are usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of installation, the log might be in `/tmp`.

8. Type 2 to specify that you want to upgrade GUI server and Device server.

**NOTE:**

- The NSM installer displays the Refresh option if the currently installed version and the version being installed are same. For example, if you install NSM 2012.2R5 on NSM 2012.2R5, the NSM installer displays the Refresh option.
- For upgrades to major release versions, the NSM installer displays the Upgrade option instead of the Refresh option. For example, if you upgrade from NSM 2010.3 to NSM 2012.2, the NSM installer displays the Upgrade option.
- For upgrades to minor release versions, the NSM installer displays the Patch option instead of the Refresh option. For example, if you upgrade from NSM 2012.2R1 to NSM 2012.2R5, the NSM installer displays the Patch option.

9. The NSM installer conducts checks for license requirement and if required, it prompts you to enter the license key file. When you enter the license key file, the NSM installer validates the license key file and stores it on the NSM server.
- The NSM installer checks the number of devices managed by the NSM, and if there are more than 25 devices, it displays a warning message about the license requirement. After you press Enter to proceed, the NSM installer displays the installation ID and the number of devices. If a license key is already available, the installer validates the existing license key. If a license key is not available, the installer prompts for the location of the license file.
 - If there are 25 or fewer devices in NSM and no license exists, the installer prompts you to use the base license.

If you enter **y** (yes), the NSM installer proceeds with the NSM upgrade. If you enter **n** (no), it displays the installation ID and number of devices in NSM and prompts you for the location of the license file.

However, if a license was already installed, the NSM installer validates it and continues with the installation.



NOTE: If the NSM installer prompts you for the license file and the license key is not available, press **Ctrl+Z** to exit the NSM installer.

For information about generating the license key, see [\[Unresolved xref\]](#).

The NSM installer script output is as follows:

```
##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if installed Device Server is newer.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
Checking device count.....ok

1) Clean install of both Device Server and GUI Server
2) Upgrade both Device Server and GUI Server from 2011.4 to 2012.2R4
Enter selection (1-2) [2]> 2

WARNING:
You are about to upgrade the server on this machine. If you need to
backup your data before continuing, abort upgrade, backup your existing
data, and then rerun this upgrade.
Please see http://kb.juniper.net/KB3603 for details.

Hit Ctrl-C to abort upgrade or ENTER to continue

Do you want to do NSM installation with base license? (y/n) [y]> n

The installation ID for this system is: 0213032010200006

Number of Devices managed by NSM is: 0

Enter the License File Path>
```



NOTE: When the iptables service is running in NSM appliances, see [KB25681](#) for more information on NSM hardening using IP tables. In NSM4000 appliances, the iptables service is enabled by default.

10. On the Device server appliance, the NSM installer prompts you to restore the NSM Profiler DB.

Do you want to restore PostgreSQL database?(y/n) [y]>



NOTE: Enter n if the NSM appliance is running on CentOS4.x.

When you type y or press Enter, the restore procedure prompts you for the file path of the NSM Profiler DB backup.

Enter PostgreSQL data backup file location [/var/netscreen/DevSvr]

11. The NSM installer prompts you to select the device schemas that need to be installed. Depending on the device models being managed by NSM, select the appropriate option. By default, all device schemas are selected.



NOTE: The NSM installer does not prompt for the steps 12 and 13 if you are patching from NSM 2012.2 to 2012.2Rx.

12. If you are upgrading NSM to a 2012.2 service release from a version earlier than 2012.2, the NSM installer displays the configured HA settings and prompts you for a one-time password for the GUI server.

Enter the one-time password for this Gui Server

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>



NOTE: The one-time password is used between the primary and secondary GUI servers for establishing a trusted connection between the two servers for database replication. Ensure that you use the same password for both the primary and the secondary appliances.

13. The NSM installer also prompts you to enter the heartbeat password for HA, which will be used by the HA server to authenticate the peer server.

Please enter shared password that will be used for Heartbeat authentication

Enter password (password will not display as you type) >

Please enter again for verification

Enter password (password will not display as you type) >



.....

NOTE: Make sure that the heartbeat password is the same for both the primary and the secondary appliances.

.....

14. The NSM installer prompts you to restart the services when the upgrade is complete.

Type **y** and press Enter to restart the servers when finished.



NOTE: Type **n** to ensure that the services do not start at the end of upgrade process. This is to ensure that the secondary appliance does not become the active node after the NSM upgrade, if the primary node is not up by the time secondary has been upgraded.

15. The NSM installer prompts you to verify your upgrade configuration settings. If the configuration settings are correct, type **y** and press Enter to proceed. If the configuration settings are incorrect, type **n** and press Enter to return to the original selection prompt.

The upgrade proceeds automatically. The NSM installer performs the following actions:

- Upgrades the Device server
- Upgrades the GUI server
- Upgrades the HA server
- Sets startup scripts

16. The NSM installer performs post-installation tasks such as removing the staging directory and starting the server processes (if configured).

The installation script logs the actions that it performs, to help in troubleshooting. At the end of the upgrade process, the NSM installer saves the log file in `/usr/netscreen/DevSvr/var/errorLog/` and provides the name of the installation log file.

17. After the successful installation, move the NSM Linux installer file to `/var/install` (example: `mv nsm2012.2R2_servers_linux_x86.sh /var/install`), and enter the following commands under `/var/install`:

- `rm -f NSM-RS`
- `ln -s <Name_of_the_Linux_build_of_service_Release.sh> NSM-RS`
- `chmod 755 NSM-RS`



NOTE: For NSM-CM appliances, enter the following commands:

- `rm -f NSM-CM`
- `ln -s <Name_of_the_CM_build_of_service_Release.sh> NSM-CM`
- `chmod 755 NSM-CM`

18. Start the HA server service on the primary server followed by the secondary server.

After the NSM upgrade, the primary and secondary databases will be out of sync. You need to wait for the secondary server to automatically synchronize with the primary server. The time it takes to synchronize the databases depends on the database size and network bandwidth.

19. Use the following command to verify that the secondary server is synchronized with the primary server:

```
#/usr/netscreen/HaSvr/utls/haStatus
```

20. Upgrade the GUI client on the computers where you have installed the UI client. See [“Upgrading the User Interface” on page 170](#) for details.
21. Launch the GUI and verify that you can connect to the upgraded GUI server.

Upgrading an NSM Appliance in an Extended HA Setup

This topic describes how to upgrade the NSM appliance in an extended HA setup (four separate appliances).

1. Perform the steps as described in [“Prerequisite Steps” on page 189](#).

In NSM Release 2012.2R1 and later releases, a generic ZIP file is available for upgrades.

The generic ZIP file is a system package that contains the latest updated packages that are required for upgrading the NSM appliance version.

A separate downloadable ZIP package for appliances is not used for service releases. Use the latest Generic Upgrade package from the [Software download site](#). The NSM installer now has the capability to modify the version information on NSM appliances.



NOTE: Perform the following steps on GUI and Device server appliances.

The files required for the offline upgrade of the NSM appliance to the NSM 2012.2 service release are listed in [Table 22 on page 219](#). The files can be downloaded from <http://www.juniper.net/customers/csc/software/>.

Table 22: Files for Offline Upgrade

Filename	Download Link
nsm_generic_offline_upgrade_CentOS4.x.zip	NSM Appliance Generic Offline Upgrade Package_vX-CentOS 4.x (X in vX represents the latest version of the generic ZIP file/generic online upgrade script.)
nsm_generic_offline_upgrade_CentOS5.x.zip	NSM Appliance Generic Offline Upgrade Package_vX-CentOS 5.x (X in vX represents the latest version of the generic ZIP file/generic online upgrade script.)
nsm2012.2RX_servers_linux_x86.zip	Linux Server (for NSM Regional Server)

**NOTE:**

- If you have already upgraded the NSM appliance to NSM version 2012.2 and want to upgrade to any release between 2012.2R1 and 2012.2R4, you can upgrade using just the Linux build of the respective service release. However, to upgrade to service releases 2012.2R5 or later, from 2012.2, use version 2 of the generic offline or online files in addition to the Linux build.
- If you have chosen online mode, you need to copy only the upgrade-os.sh file from the NSM Appliance Generic Online Upgrade Script_vX' (X represents the version of the generic online upgrade script) link on the [Juniper Networks website](#) along with the desired 2012.2 Linux build to the NSM appliance.

2. Copy the following files to your NSM appliance using FTP or SCP:
 - **nsm_generic_offline_upgrade_CentOS4.x.zip:** Offline mode for CentOS 4.X
 - **nsm_generic_offline_upgrade_CentOS5.x.zip:** Offline mode for CentOS 5.7
 - **nsm2012.2RX_servers_linux_x86.zip** (X in 2012.2RX represents the required version of the Linux Server Installer for NSM).
3. Unzip the required file using the **unzip** `<Name_of_the_generic_offline_upgrade_on_OS_version.zip>` command, on the NSM appliance.

Example: **unzip nsm_generic_offline_upgrade_CentOS5.x.zip**
4. Extract the latest NSM 2012.2 service release Linux build using the **unzip** `<Name_of_the_Linux_build_of_service_Release.zip>` command, on the NSM appliance.

Example: **unzip nsm2012.2R2_servers_linux_x86.zip**

5. First, stop the service of HA servers on the appliances that are in the standby state, and then stop the service of HA servers on the appliances that are in the active state. Use the `/usr/netscreen/HaSvr/utls/haStatus` command to identify the state of the appliances. Ensure that they are in sync.

To stop HA servers, use the following command:

```
/etc/init.d/haSvr stop
```

6. Identify the appliances that are configured as primary servers and the appliances that are configured as secondary servers by checking the IP addresses configured for the `highAvail.primaryServerIp` and `highAvail.secondaryServerIp` parameters in `/usr/netscreen/HaSvr/var/haSvr.cfg`.

7. To start the upgrade, run the `sh upgrade-os.sh` `<Name_of_the_Linux_build_of_service_Release.sh> Offline/Online` command on primary servers (identified in step 6) and then run the command on secondary servers.

Example: To perform an offline upgrade to NSM2012.2R2, run the `sh upgrade-os.sh nsm2012.2R2_servers_linux_x86.sh Offline` command.

To perform an online upgrade to NSM2012.2R2, run the `sh upgrade-os.sh nsm2012.2R2_servers_linux_x86.sh Online` command.

The `upgrade-os.sh` script prompts you to back up the NSM Profiler DB. Later, the NSM installer uses the NSM Profiler DB backup to restore the data.



NOTE: The `upgrade-os.sh` file prompts you for the NSM Profiler DB backup only if the NSM appliance is running CentOS 5.7.

The `upgrade-os.sh` script updates the system packages and runs the NSM installer. The NSM installer begins a series of pre-installation checks that ensures:

- You are installing the correct software for your operating system.
- All the necessary software binaries are present.
- You have correctly logged in as root user.
- You have installed a version of NSM earlier than the current version you are installing.
- The system has sufficient disk space and RAM.

**NOTE:**

- **Done** indicates that the NSM installer has successfully performed a task.
- **OK** indicates that the NSM installer has performed a check and verified that the condition was satisfied.
- **FAILED** indicates that the NSM installer performed a task or check, but it was not successful. See the install log for information about the failure.

This log is usually stored in `/usr/netscreen/DevSvr/var/errorLog`. If the failure happens in the early stages of installation, the log might be in `/tmp`.

8. Type **3** to specify that you want to upgrade only the GUI server or only the Device server.

**NOTE:**

- The NSM installer displays the **Refresh** option if the currently installed version and the version being installed are same. For example, if you install NSM 2012.2R5 on NSM 2012.2R5, the NSM installer displays the **Refresh** option.
- For upgrades to major release versions, the NSM installer displays the **Upgrade** option instead of the **Refresh** option. For example, if you upgrade from NSM 2010.3 to NSM 2012.2, the NSM installer displays the **Upgrade** option.
- For upgrades to minor release versions, the NSM installer displays the **Patch** option instead of the **Refresh** option. For example, if you upgrade from NSM 2012.2R1 to NSM 2012.2R5, the NSM installer displays the **Patch** option.

9. The NSM installer conducts checks for license requirement and if required, it prompts you to enter the license key file. When you enter the license key file, the NSM installer validates the license key file and stores it on the NSM server.

- The NSM installer checks the number of devices managed by NSM, and if there are more than 25 devices, it displays a warning message about the license requirement.

After you press Enter to proceed, the NSM installer displays the installation ID and the number of devices. If a license key is already available, the installer validates the existing license key. If a license key is not available, the installer prompts for the location of the license file.

- If there are 25 or fewer devices in NSM and no license exists, the installer prompts you to use the base license.

If you enter **y** (yes), the NSM installer proceeds with the NSM upgrade. If you enter **n** (no), it displays the installation ID and number of devices in NSM and prompts

for the location of license file. However, if a license was already installed, the NSM installer validates it and continues with the installation.



NOTE:

- This step is applicable only for GUI server.
- If the NSM installer prompts you for the license file and the license key is not available, press Ctrl+Z to exit the NSM installer.

The NSM installer script output for the Device server is as follows:

```
##### PERFORMING PRE-INSTALLATION TASKS #####
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
Checking if iptables is running.....ok
Checking if installed Device Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
1) Patch Device Server from 2012.2R5 to 2012.2R6, install GUI Server
2) Clean install of Device Server, install GUI Server
3) Patch Device Server only from 2012.2R5 to 2012.2R6
4) Clean install of Device Server only
Enter selection (1-4) [3]>

WARNING:
You are about to upgrade the server on this machine. If you need to
backup your data before continuing, abort upgrade, backup your existing
data, and then rerun this upgrade.
Please see http://kb.juniper.net/KB3603 for details.

Hit Ctrl-C to abort upgrade or ENTER to continue

Select Device Schema to be loaded in NSM

1) Load all Device Family Schemas
2) Load Screen OS Device Schema only (Screen OS)
3) Load Screen OS and J/SRX Devices Schema only (Screen OS + J/SRX Series)
```

```

Enter selection (1-3)[1]> 3
##### POST-INSTALLATION OPTIONS #####

Start High Availability daemon processes when finished? (y/n) []> n

##### CONFIRMATION #####

About to proceed with the following actions:
- Patch Device Server
- Patch High Availability Server
- ScreenOs and J/SRX Device Family Schemas Load
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n)> n

```



NOTE: When the iptables service is running in NSM appliances, see [KB25681](#) for more information on NSM hardening using IP tables. In NSM4000 appliances, the iptables service is enabled by default.

10. On the Device server appliance, the NSM installer prompts you to restore the NSM Profiler DB.

Do you want to restore PostgreSQL database?(y/n) [y]>



NOTE: Enter n if the NSM appliance is running on CentOS4.x.

When you type y or press Enter, the restore procedure prompts you for the file path of the NSM Profiler DB backup.

Enter PostgreSQL data backup file location [/var/netscreen/DevSvr]

11. On both the GUI and Device server appliances, the NSM installer prompts you to select the device schemas to be installed. Depending on the device models being managed by NSM, select the appropriate option. By default, all device schemas are selected.



NOTE: The NSM installer does not prompt for the steps 12 and 13 if you are patching from NSM 2012.2 to 2012.2Rx.

12. If you are upgrading NSM to a 2012.2 service release from a version earlier than 2012.2, the NSM installer displays the configured HA settings and prompts you for a one-time password on the GUI server.

Enter the one-time password for this Gui Server

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>



NOTE: The one-time password is used between the primary and secondary GUI servers for establishing a trusted connection between the two servers for database replication. Ensure that you use the same password for both the primary and the secondary appliances.

13. The NSM installer also prompts you to enter the heartbeat password for HA, which will be used by the HA server to authenticate the peer server.

Please enter shared password that will be used for Heartbeat authentication

Enter password (password will not display as you type) >

Please enter again for verification

Enter password (password will not display as you type) >



NOTE: Make sure that the heartbeat password is the same for both the primary and the secondary appliances.

14. The NSM installer prompts you to restart the services when the upgrade is complete. Type **y** and press Enter to restart the servers when finished.



NOTE: Type **n** to ensure that the services do not start at the end of upgrade process. This is to ensure that the secondary appliance does not become the active node after the NSM upgrade, if the primary node is not up by the time secondary has been upgraded.

15. The NSM installer prompts you to verify your upgrade configuration settings.

If the settings are correct, type **y** and press Enter to proceed. If settings are incorrect, type **n** and press Enter to return to the original selection prompt.

The upgrade proceeds automatically. The NSM installer performs the following actions:

- Upgrades the Device server or the GUI server
- Upgrades the HA server
- Sets startup scripts

16. The NSM installer performs post-installation tasks such as removing the staging directory and starting the server processes (if configured).

The installation script logs the actions that it performs, to help in troubleshooting. At the end of the upgrade process, the NSM installer provides the name and location of the installation log file.

**NOTE:**

- If only the GUI server is upgraded, the log file is saved in `/usr/netscreen/GuiSvr/var/errorLog/`.
- if only the Device server is upgraded, the log file is saved in `/usr/netscreen/DevSvr/var/errorLog/`

17. After the successful installation, move the NSM Linux installer file to `/var/install` (example: `mv nsm2012.2R2_servers_linux_x86.sh /var/install`), and enter the following commands under `/var/install`:

- `rm -f NSM-RS`
- `ln -s <Name_of_the_Linux_build_of_service_Release.sh> NSM-RS`
- `chmod 755 NSM-RS`

18. Start the HA server service on the primary GUI and primary Device servers followed by the HA server service on the secondary GUI and secondary Device servers.

After the NSM upgrade, the database will be out of sync on the secondary GUI server. You need to wait for the secondary server to automatically synchronize with the primary server. The time it takes to synchronize the databases depends on the database size and network bandwidth.

19. Run the following command to verify that the secondary server is synchronized with the primary server:

```
#/usr/netscreen/HaSvr/utlis/haStatus
```

20. Upgrade the GUI client on the computers where you have installed the UI client. See [“Upgrading the User Interface” on page 170](#) for details.

21. Launch the GUI and verify that you can connect to the upgraded GUI server.

Migrating Data to an NSM Regional Server Appliance

This section provides information on how to port data from a Solaris server or a Linux server running NSM to an NSMXpress or NSM3000 appliance. It contains the following procedures:

- [Data Migration from a Solaris Server to an NSM Regional Server Appliance on page 225](#)
- [Data Migration from a Linux Server to an NSM Regional Server Appliance on page 228](#)

Data Migration from a Solaris Server to an NSM Regional Server Appliance



NOTE: The existing traffic logs on the Solaris server are not compatible with NSMXpress and cannot be migrated. Only the GUI server database can be migrated.

On the Solaris server:

1. Upgrade the Solaris server to the latest NSM release, or to the release that you will use on the NSM appliance.

2. Stop the NSM processes:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

3. Run the exporter.

These commands assume that `/var/netscreen/GuiSvr` is your GUI server data directory. If not, then replace `/var/netscreen/GuiSvr` with the path to your GUI server data directory.

Use these commands to run the exporter:

```
rm -f /tmp/xdBExporter.pid
/usr/netscreen/GuiSvr/Utils/xdBExporter.sh /var/netscreen/GuiSvr/xdB
/var/netscreen/GuiSvr/csvfile.txt
```

4. Use FTP to copy `csvfile.txt` to a common location.

On the NSM appliance:

1. Use the `nsm_setup` utility to:
 - a. Change the IP address, netmask, and gateway of the NSM appliance server to those of the Solaris server, if you need to use the same IP configuration in NSMappliance.
 - b. Perform a clean installation of the latest release of NSM on the NSM appliance, or install the same release you installed on the Solaris server.



NOTE: The version of NSM on the NSM appliance server and the Solaris server must match exactly.

2. Use FTP to copy the `csvfile.txt` to `/var/netscreen/GuiSvr`.
3. Log in as an `nsm` user by entering the following command, and then enter the admin password:

```
sudo su - nsm
```

4. Stop the HA server, GUI server, and Dev server processes with the following commands:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

5. Run Importer using the following command:

```
/usr/netscreen/GuiSvr/Utils/xdifImporter.sh /var/netscreen/GuiSvr/csvfile.txt
/var/netscreen/GuiSvr/xdb/init
```

6. Run **xdbViewEdit** using the following command. Set the path of vi editor to **/bin/vi**:

```
/usr/netscreen/GuiSvr/Utils/.xdbViewEdit.sh
```



CAUTION: You are about to edit your database. Editing errors could corrupt your data. The commands you will use are the same as in the vi editor. If you are not familiar with vi, get assistance.

7. Change the IP address in the server table to that of the NSM appliance: Option 70.server.00.server.1

```
[nsm@NSMExpress ~]$ /usr/netscreen/GuiSvr/Utils/.xdbViewEdit.sh
Start XDB View Editor in read-only mode? [y]/n: n.
.
.
Please enter path to editor [/usr/bin/vi]: /bin/vi
xdb editor set to /bin/vi
Hit ENTER or return to continue...

Hit ENTER or return to continue...
  1. Display all domains with domain-id
  2. Display all category names
  3. Display tuples in a category across all domains
  4. Display tuples in a category for a single domain
  5. View/Edit record by category.doc-id
  6. View/Edit record by domain-id.category.tuple-name
  7. View/Edit record by domain-id.category.tuple-id
  8. View Reference DB
  9. Change DB version (Disabled in RW mode)
 10. Insert a record by domain-id.category
 11. Delete a record by domain-id.category.tuple-id
 12. Quit

      Enter choice number: 7
Enter tuple-name in format domain-id.category.tuple-id: 0.server.0

<Esc>:wq to write and quit.
<Esc>:q! to just quit and not write.
```

8. View and make note of the client one-time password in the `shadow_server` table:
Option 70.shadow_server.1

```
<Esc>:q! to just quit and not write
```

9. Exit the `xdbViewEdit.sh` editor.
10. Change the one-time password in `devSvr.cfg` to match the one-time password in the `shadow_server` table:
 - a. Use the vi editor to edit the `/var/netscreen/DevSvr/devSvr.cfg` file.
 - b. Change the one-time password to match the one-time password from the `shadow_server` table.
 - c. Delete the `ourRsaPrivateKey` and `theirRsaPublicKey` lines in `devSvr.cfg`.
11. Start the HA server, GUI server, and Device server processes by entering the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

Data Migration from a Linux Server to an NSM Regional Server Appliance

This section describes porting data from an existing Linux server to an NSM appliance. This section makes the following assumptions:

- The IP address of the existing Linux server will be assigned to the new NSM appliance server.
- The versions of NSM are the same on the current Linux installation and the NSM appliance. If the versions are different, you must upgrade the Linux server to the NSM version that is running on the NSM appliance before migrating your data.

On the Linux Server

1. Upgrade the Linux server to the latest NSM release, or to the release that you will use on the NSM appliance.
2. Stop the NSM processes:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop  
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop  
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

3. Enter the following commands to back up the NSM database from GuiSvr to the `Guidb.tar` archive file. These commands assume `/var/netscreen/GuiSvr` is your GUI server data directory.

```
cd /var/netscreen
tar cvf Guidb.tar GuiSvr
```

4. If you want device logs and the Device server data directory to be migrated, execute the following commands to back up the NSM database from DevSvr to the **Devdb.tar** archive file.



NOTE: The device log files are often large, so migration might not be practical.

```
cd /var/netscreen
tar cvf Devdb.tar DevSvr
```

5. Transfer the **Guidb.tar** and **Devdb.tar** archive files to a place where they can be retrieved later.

On the NSMAppliance

1. Use the **nsm_setup** utility to:
 - a. Change the IP address, netmask, and gateway of the NSM appliance server to those of the Linux server, if you need to use the same IP configuration in the NSM appliance.
 - b. Perform a clean installation of the latest NSM release, or to the release you have on the Linux server.

2. Enter the following command and the admin password to gain root access:

```
sudo su -
```

3. Stop the NSM server processes:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

4. To avoid conflicts between the NSM appliance **xdb** database and the database in **Guidb.tar**, delete the **xdb** subdirectory:

```
cd /var/netscreen
rm -rf GuiSvr/xdb/
```

5. Copy the **Guidb.tar** and **Devdb.tar** archive files to **/var/netscreen**.

6. Extract the database:

```
cd /var/netscreen ; tar xvpf Guidb.tar
cd /var/netscreen ; tar xvpf Devdb.tar
```

7. Log in as the nsm user by entering the following command and using the admin password:

```
sudo su - nsm
```



NOTE: If you are not using the same IP address in the NSM appliance as you had for the Linux server, follow steps 6, 7, and 9 of the procedure for migrating data from Solaris to an NSM appliance. See [“On the NSM appliance:” on page 226](#).

Also make sure that the guiSvrX.addr details in the /var/netscreen/DevSvr/devSvr.cfg file are correct.



NOTE: If you are migrating only the GUI server data directory to the NSM appliance, follow steps 6, 8, 9, and 10 of the procedure for migrating data from Solaris to an NSM appliance. See [“On the NSM appliance:” on page 226](#).

These steps are required:

- Delete the existing RSA keys between devSvr and guiSvr from the devSvr.cfg file so they can be renegotiated and established again.
- Correct the one-time client password in devSvr.cfg.

8. If the Linux server used a customized device server data directory, then you must open the /var/netscreen/pgsql/data/postgresql.conf file on the NSM appliance and change the **?data directory?** config parameter from the customized path used on the Linux server to the default /var/netscreen/DevSvr/ before starting the NSM server processes.

9. Start the HA server, GUI server, and Dev server processes:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

User Privileges on an NSM Appliance

The NSM appliance allows you to execute commands with root privileges or nsm privileges and to switch back and forth.

- Log in as admin and execute the **sudo su - nsm** command any time you want to run an NSM-specific command, such as starting or stopping a service manually or running a CLI command.

- Log in as admin and execute the **sudo su -** command any time you want to reboot or shut down.
- Log in as admin to run the **nsm_setup** utility to configure various system settings and to install Regional Server or Central Manager.

The following procedure assumes you have initially logged in using admin.

To change user privileges from user to admin:

1. Log in as an nsm user by entering the following command at the prompt:

```
[admin@NSMXpress ~]$ sudo su - nsm  
Password: [admin password]
```

2. Change user privileges to admin by entering the following command at the prompt.

```
[nsm@NSMXpress ~]$exit
```

3. Change to root by entering the following command at the prompt.

```
[admin@NSMXpress ~]$sudo su -  
Password:[admin password]
```


CHAPTER 7

Upgrading CentOS 4.x to CentOS 5.7 on NSM Appliances

To resolve some security vulnerabilities in CentOS 4.X releases, from NSM 2012.1 onwards you need to upgrade NSM appliances to CentOS 5.7. NSM 2011.4 and 2010.3 can also run on CentOS 5.7. This section shows you how to upgrade your existing NSMXpress appliances to run CentOS 5.7.

- [Upgrading an NSM Appliance OS on page 233](#)
- [Setting Up Administrative Accounts and Networking on page 236](#)
- [Tested CentOS Upgrade Paths on page 245](#)

Upgrading an NSM Appliance OS

This section shows you how to use RIT server mechanism using local hard disk.

Upgrade Using Local Hard disk

To upgrade CentOS 4.x to CentOS to 5.7 using upgrade script:

1. Download the script [Update Recovery Partition for CentOS 5.7](#) to the NSM Appliance **/tmp** directory.
2. Download [CentOS 5.7 ISO image](#) to the NSM Appliance **/tmp** directory.
3. Extract the **CentOS5.7_servers_upgrade_ISO.iso** file using the command **# unzip /tmp/CentOS5.7_servers_upgrade_ISO.zip**.

Example:

```
[root@NSMXpress tmp]# unzip /tmp/CentOS5.7_servers_upgrade_ISO.zip
Archive: CentOS5.7_servers_upgrade_ISO.zip
inflating: CentOS5.7_servers_upgrade_ISO.iso
```

4. Execute the downloaded script with CentOS 5.7 ISO image using the command **# sh /tmp/updateRecoveryPartition_5.7.sh/tmp/CentOS5.7_servers_upgrade_ISO.iso**.

Example:

```
[root@NSMXpress tmp]# sh /tmp/sdaboot-mpModv2.sh
/tmp/CentOS5.7_servers_upgrade_ISO.iso
--- Running sdaboot-mpModv2.sh ---
Creating Mount directory.....OK
Checking /var/cores disk space.....OK
Checking Mount for CentOS5.7_servers_upgrade_ISO.isoOK
Checking Mount for sda1.....OK
Mounting /dev/sda1.....OK
Mounting CentOS5.7_servers_upgrade_ISO.iso.....OK
Backing up existing BOOTLOADER.....OK
Replacing sda1 boot modules with CentOS5.7_servers_upgrade_ISO.isoOK
Replacing nsm.iso in sda1.....OK
Copying ks.cfg upgrade ISO to HD.....OK
Modifying ks.cfg to boot from HD.....OK
Modifying Grub Menu.....OK
Unmounting sda1.....OK
Unmounting CentOS5.7_servers_upgrade_ISO.iso.....OK
System is ready for REBOOT
```

5. Disable all the ports of NSM Appliance.

The ports to be disabled are:

- eth0
- eth1
- eth2
- eth3

6. Reboot the NSM Appliance.
7. During reboot process, press any key to enter the menu when prompted.

A menu screen with the following options are displayed:

- NSMXpress
- Rescue
- Upgrade OS to Centos 5.7
- Boot from USB to restore Previous OS (Now Booting Normally)



NOTE: For NSMXpress the last option is Boot from Secondary Drive To Restore Original OS.

8. Select **Upgrade OS to CentOS 5.7** option and press **Enter**. The following is displayed:

Example:

```
Using this option will Upgrade the OS to CentOS 5.7 To confirm upgrade, type
upgrade at the password prompt. To abort and boot at the Rescue mode, just hit
<Enter> at the password prompt. Press any key.
```

9. Press any key for the password prompt.
10. Enter the password as **upgrade** and press **Enter**.

The CentOS upgrade process starts.

11. Enter **username**, **password**, and configure the **IP**, **subnet mask** and, **default gateway addresses**.

The upgrade process will take approximately 15 minutes to upgraded to CentOS 5.7 successfully.

Upgrading Using CDROM

To reimage an appliance using CDROM:

1. Download the ISO file from https://download.juniper.net/software/nsm/2012.2/CentOS5.7_servers_upgrade_ISO.zip, on a PC or Server having a DVD writer.
2. Extract the **CentOS5.7_servers_upgrade_ISO.zip** file using the command:
unzip /tmp/CentOS5.7_servers_upgrade_ISO.zip.

```
[root@NSMXpress tmp]# unzip /tmp/CentOS5.7_servers_upgrade_ISO.zip
Archive: CentOS5.7_servers_upgrade_ISO.zip
inflating: CentOS5.7_servers_upgrade_ISO.iso
```

3. Use a DVD burning tool to burn the image on a DVD.
4. Use an external USB DVD ROM drive for NSMXpress Series II or NSM3000 appliance.
5. Change the boot sequence in the BIOS to boot from the USB DVD ROM drive
6. Reboot the system.

When the system boot from DVD the following grub options are displayed:

- **rescue**
- **erase-reinstall**
- **memtest86**

7. Select **erase-reinstall** and let the automated installation complete.
8. Refresh NSM and interface configuration after automated the installation.

Setting Up Administrative Accounts and Networking

Logging In to the System

- Log in as an administrator using the password **abc123**, and change the password when prompted.

Connecting an Appliance to the Network

To connect an NSM appliance to the network, follow the prompts as displayed in the console:

- Please enter new IP address for interface eth0
Enter the value **10.205.10.161**.
- Please enter new subnet mask for interface eth0
Enter the value **255.255.0.0**.
- Enter the default gateway as a dotted-decimal IP address:
Enter the value **10.205.10.161**.



NOTE:

- The values used are examples.
- If you enter an incorrect value, a message appears that directs you to enter your responses in dotted-decimal format.
- To configure your system with a web browser, connect to <https://10.205.10.161/administration>.

Configuring and Installing NSM

To configure and install NSM:

1. Log in as a root user.
When you are prompted for a password, provide the administrator password you set previously in “Logging In to the System” on page 236.
2. Create a directory to copy the build using the command **mkdir/var/install**.
3. Move the build from the directory **/usr** or copy the build to **/var/install/**.
4. Change the permissions inside **/var/install/** using the command **chmod 755 <NSM build>**.
5. Create a new softlink in the **/var/install/** directory using the command **ln -s <NSM build.sh>NSM-RS** for the Regional Server and **ln -s <NSM build.sh>NSM-CM** for the Central Manager.

Running NSM Setup

Use the **nsm_setup** command to install NSM and set up the regional server. The menu options available are:

```
1> Change Password
2> Set Interfaces
3> Set Routing
4> Change Hostname
5> Set DNS Servers
6> Change Time Options
7> Forward Local Status Emails
8> System Security Update
9> Reconfigure NSM Regional Server

Q> Quit
R> Redraw menu

Choice [1-9,Q,R]:
Q> Quit
R> Redraw menu
```

Sub Option Choice [1-10,Q,R]: 5

```
DNS name server options:
1> Add a nameserver
2> Delete 10.206.194.50

M> Return to Main Menu
R> Redraw menu

Choice [1-2,M,R]: 1
Please type the new nameserver in dotted decimal notation:
10.206.194.50
```

Sub Option Choice [1-9,Q,R]: 9

When you select option 9, Reconfigure NSM Regional Server, the following sub-options are available. Select option 1 to view the typical settings.

```
Applying system changes before processing NSM changes.
Note: after running NSM configuration, the setup utility will exit.

1> Typical Settings
2> Custom Settings

Q> Quit
R> Redraw menu
```

Sub Option Choice 1 - Typical Setting

When you select option 1, Typical Settings, the following sub-options are available. Select option 2 to configure the administrative password:

```
NSM Configuration Main Menu

1> Management IP [10.205.10.161]
   The IP address on this server that will be
   used for management

2> NSM 'super' password []
   Password for 'super' user

3> GUI server one-time password []
   Password to initiate authentication
   between HA peers and to Central Manager.
   This password must be the same for all
   NSM servers in this installation.

4> Cfmuser password []
   CfmPassword for ConfigFileVersions directory

5> NSM License type []
   Specify a license file, or select "Base Install"
   to use the built-in limited device license.

6> FIPS Support [n]
   Enable FIPS Support or not

A> Apply settings
C> Cancel all changes and quit
R> Redraw menu
```

Choice [1-6,A,C,R]: 2

When you select option 2, Custom Settings, the following sub-options are available. Select option 3 to configure the GUI server one-time password.

```
Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>
Password set!

SM Configuration Main Menu

1> Management IP [10.205.10.161]
   The IP address on this server that will be
   used for management

2> NSM 'super' password [*****]
   Password for 'super' user

3> GUI server one-time password []
```

```

Password to initiate authentication
between HA peers and to Central Manager.
This password must be the same for all
NSM servers in this installation.

4> Cfmuser password []
   CfmPassword for ConfigFileVersions directory

5> NSM License type []
   Specify a license file, or select "Base Install"
   to use the built-in limited device license.

6> FIPS Support [n]
   Enable FIPS Support or not

A> Apply settings
C> Cancel all changes and quit
R> Redraw menu

```

Choice [1-6,A,C,R]: 3

When you select option 3, GUI server one-time password, the following sub-options are available:

```

Password to initiate authentication between HA peers and to Central Manager. This
password must be the same for all NSM servers in this installation.
Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>
Password set!

NSM Configuration Main Menu

1> Management IP [10.205.10.161]
   The IP address on this server that will be
   used for management

2> NSM 'super' password [*****]
   Password for 'super' user

3> GUI server one-time password [*****]
   Password to initiate authentication
   between HA peers and to Central Manager.
   This password must be the same for all
   NSM servers in this installation.

4> Cfmuser password []
   CfmPassword for ConfigFileVersions directory

5> NSM License type []
   Specify a license file, or select "Base Install"
   to use the built-in limited device license.

6> FIPS Support [n]
   Enable FIPS Support or not

```

```
Apply settings
C> Cancel all changes and quit
R> Redraw menu
```

Choice [1-6,A,C,R]: 4

When you select option 4, Cfmuser password, the following sub-options are available:

```
CfmPassword for ConfigFileVersions directory
Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>
Password set!

NSM Configuration Main Menu

1> Management IP [10.205.10.161]
   The IP address on this server that will be
   used for management

2> NSM 'super' password [*****]
   Password for 'super' user

3> GUI server one-time password [*****]
   Password to initiate authentication
   between HA peers and to Central Manager.
   This password must be the same for all
   NSM servers in this installation.

4> Cfmuser password [*****]
   CfmPassword for ConfigFileVersions directory

5> NSM License type []
   Specify a license file, or select "Base Install"
   to use the built-in limited device license.

6> FIPS Support [n]
   Enable FIPS Support or not

A> Apply settings
C> Cancel all changes and quit
R> Redraw menu
```

Choice [1-6,A,C,R]: 5

When you select option 5, NSM License type, the following sub-options are available:

```
1> Base Install
2> Select License File

M> Main Menu
R> Redraw menu
```

Choice [1-2,M,R]: 1

When you select option 1, Base Install, the following sub-options are available:

```
NSM Configuration Main Menu

1> Management IP [10.205.10.161]
   The IP address on this server that will be
   used for management

2> NSM 'super' password [*****]
   Password for 'super' user

3> GUI server one-time password [*****]
   Password to initiate authentication
   between HA peers and to Central Manager.
   This password must be the same for all
   NSM servers in this installation.

4> Cfmuser password [*****]
   CfmPassword for ConfigFileVersions directory

5> NSM License type [Base_Install]
   Specify a license file, or select "Base Install"
   to use the built-in limited device license.

6> FIPS Support [n]
   Enable FIPS Support or not

A> Apply settings
C> Cancel all changes and quit
R> Redraw menu
```

Choice [1-6,A,C,R]: A

When you select option A, Apply settings, the installation process runs and displays the following output.

```
Stopping NFS statd: [FAILED]
Starting NFS statd: [ OK ]

##### PERFORMING PRE-INSTALLATION TASKS #####
==> Setting Staging Directory to /var/tmp
Creating staging directory...ok
Running preinstallcheck...
Checking if platform is valid.....ok
Checking for correct intended platform.....ok
Checking for CPU architecture.....ok
Checking if all needed binaries are present.....ok
Checking for platform-specific binaries.....ok
Checking for platform-specific packages.....ok
skipped
Checking in System File for PostgreSQL and XDB parameters...ok
Checking for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user nsm exists.....ok
```

```

Checking if iptables is running.....ok
Checking if installed Device Server is newer.....ok
Checking if installed GUI Server is newer.....ok
Checking if installed HA Server is newer.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Noting OS name.....ok
Stopping any running servers

##### EXTRACTING PAYLOADS #####
Extracting and decompressing payload.....ok
Extracting license manager package.....ok

##### GATHERING INFORMATION #####
Checking device count.....ok

1) Clean install of both Device Server and GUI Server
2) Refresh both Device Server and GUI Server
==> Set to action UDS-UGS

Base install: set to y

Number of Devices managed by NSM is: 0
##### GENERAL SERVER SETUP DETAILS #####

Will this machine participate in an HA cluster? (y/n) [n]>
==> Set to n

##### DEVICE SERVER SETUP DETAILS #####

##### GUI SERVER SETUP DETAILS #####

==> Management IP set to 10.205.10.161

==> NBI port set to 8443

Please enter a password for the 'super' user
==> Hashed password set to glee/aW9b0YEewkD/6Ri8sHh2mU=

==> Set GUI Server one-time password

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]>==> Set
to n

==> CFM user is set to 'cfmuser'

==> CFM password set for 'cfmuser'

##### HIGH AVAILABILITY (HA) SETUP DETAILS #####

Automatic restarts of servers? (y/n) [y]>
==> Set to y

##### BACKUP SETUP DETAILS #####

Will this machine require local database backups? (y/n) [y]>
==> Set to y

==> Setting start hour for database backup to 02

```

```

Will daily backups need to be sent to a remote machine? (y/n) [n]>
==> Set to n

Enter number of database backups to keep. The default value will keep the last
seven backups.
The oldest backup copy will be overwritten by the new backup copy [7]>
==> Set number of database backups to keep to 7

Enter the rsync backup timeout [1800]>
==> Set to 1800

Enter database backup directory [/var/netscreen/dbbackup]>
==> Setting database backup directory to /var/netscreen/dbbackup
WARNING: Directory /var/netscreen/dbbackup already exists.
Existing backups in this directory may not be
compatible with this new software.
Please exit installation and move the contents
as they will get WIPED OUT during installation.

##### DEVSVR DB SETUP DETAILS #####

==> Postgres DevSvr Db port set to 5432

==> Postgres DevSvr Db super user set to 'nsm'

==> Postgres DevSvr Db password set for 'nsm'

##### POST-INSTALLATION OPTIONS #####

Start server(s) when finished? (y/n)
==> Set to y

##### CONFIRMATION #####

About to proceed with the following actions:
- Refresh Device Server
- Refresh GUI Server
- Refresh High Availability Server
- This machine will have base license with maximum 25 devices
- This machine does not participate in an HA cluster
- Set password for 'super' user
- CFM user: cfmuser
- CFM Password set for 'cfmuser'
- Servers will be restarted automatically in case of a failure
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- HA rsync command backup timeout: 1800
- Create database backup in /var/netscreen/dbbackup
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: nsm
- Postgres DevSvr Db password set for 'nsm'
- Start server(s) when finished: Yes

Skipping confirmation

##### PERFORMING INSTALLATION TASKS #####

----- REFRESH Device Server -----

```

```

Putting NSROOT into start scripts.....ok
Installing JRE.....ok
Installing GCC.....ok
Refresh of DevSvr complete.

----- REFRESH GUI Server -----
Putting NSROOT into start scripts.....ok
Installing JRE.....ok
Installing GCC.....ok
ok
Updating GuiSvr Database.....ok
Refresh of GuiSvr complete.

----- REFRESH HA Server -----
Putting NSROOT into start scripts.....ok
Adding highAvail.isFailOverEnabled.....ok
Filling in HA Server config file(s).....ok
Refresh of HaSvr complete.

----- SETTING START SCRIPTS -----
Enabling Device Server start script.....ok
Enabling GUI Server start script.....ok
Enabling HA Server start script.....ok

##### PERFORMING POST-INSTALLATION TASKS #####
Deleting Unwanted Schemas.....ok
/bin/cp: cannot stat `/usr/netscreen/GuiSvr/var/metadata_table.nml': No such file
or directory
/var/install/NSM-RS: line 4462: /usr/netscreen/GuiSvr/var/tablelist: No such file
or directory
ok
Removing staging directory.....ok
Starting GUI Server.....ok
Starting Device Server.....ok
Starting HA Server.....ok

NOTES:
- Installation log is stored in
  /usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20110713224725
- Please note that TCP port 7808 is being used for server-UI communication

```



NOTE: When only CentOS upgrade is performed, NSMXpress GUI displays only the main release version. For example: 2010.3s3 will be displayed as 2010.3. This issue does not exist on 2011.4s3, 2010.3s6, and 2012.2s1 onwards.

Checking the Installation

Check if the build is installed and running. The sample out is as mentioned below:

```

[root@NSMXpress ~]# /etc/init.d/guiSvr status
[root@NSMXpress ~]# /etc/init.d/devSvr status
[root@NSMXpress ~]# /etc/init.d/devSvrversion
[root@NSMXpress ~]# /etc/init.d/guiSvr version

```

```

=====
[root@NSMXpress ~]# /etc/init.d/guiSvr status
nsm owner is nsm
Retrieving status...
guiSvrManager (pid 24588).....ON
guiSvrMasterController (pid 24766).....ON
guiSvrDirectiveHandler (pid 24969).....ON
guiSvrLicenseManager (pid 25223).....ON
guiSvrStatusMonitor (pid 25387).....ON
guiSvrWebProxy (pid 25599).....ON
[root@NSMXpress ~]# /etc/init.d/devSvr status
nsm owner is nsm
Retrieving status...
devSvrDbSvr (pid 25936).....ON
devSvrManager (pid 26095).....ON
devSvrLogWalker (pid 26253).....ON
devSvrDataCollector (pid 26434).....ON
devSvrDirectiveHandler (pid 26662).....ON
devSvrProfilerMgr (pid 26924).....ON
devSvrStatusMonitor (pid 28084).....ON
[root@NSMXpress ~]# /etc/init.d/devSvr version
nsm owner is nsm
Retrieving version information...
devSvrDbSvr PostgreSQL 8.1.7
devSvrManager 2009.1r1a (Build LGB12z1a15)
devSvrLogWalker 2009.1r1a (Build LGB12z1a15)
devSvrDataCollector 2009.1r1a (Build LGB12z1a15) 11/06/09
devSvrDirectiveHandler 2009.1r1a (Build LGB12z1a15) 11/06/09
devSvrProfilerMgr 2009.1r1a (Build LGB12z1a15)
devSvrStatusMonitor 2009.1r1a (Build LGB12z1a15)
[root@NSMXpress ~]# /etc/init.d/guiSvr version
nsm owner is nsm
Retrieving version information...
guiSvrManager 2009.1r1a (Build LGB12z1a15)
guiSvrMasterController 2009.1r1a (Build LGB12z1a15) 11/06/09
guiSvrDirectiveHandler 2009.1r1a (Build LGB12z1a15) 11/06/09
guiSvrLicenseManager 2009.1r1a (Build LGB12z1a15) 11/06/09
guiSvrStatusMonitor 2009.1r1a (Build LGB12z1a15)
guiSvrWebProxy 2009.1r1a (Build LGB12z1a15) 11/06/09
[root@NSMXpress ~]#

```

Tested CentOS Upgrade Paths

The upgrade scenarios requires the following components:

- ISO image
- Centos 4.x -2012.1 zip files
- Centos 5.7-2012.1 zip files
- Linux builds of main and patch releases as mentioned in the scenarios.

Scenarios available for CentOS upgrade on NSM 3000 and NSM Series II appliances are:

- [Scenario 1 on page 246](#)
- [Scenario 2 on page 246](#)

- [Scenario 3 on page 246](#)
- [Scenario 4 on page 247](#)
- [Scenario 5 on page 247](#)
- [Scenario 6 on page 247](#)
- [Scenario 7 on page 247](#)
- [Scenario 8 on page 248](#)
- [Scenario 9 on page 248](#)
- [Scenario 10 on page 249](#)

Scenario 1

2009.1r1a (CentOS 4.x) to 2010.3s4(CentOS 4.X) through ISO to 2010.3s4nsm2012.1_servers_upgrade_rs_5.7.zip

The purpose of this scenarios is to check if CentOS upgrade works for 2010.3s4. This scenario covers the following:

- Migration from 2009.1.r1a (SAM) build having 4.x CentOS version to 2010.3s4 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.

Scenario 2

2009.1r1a (CentOS 4.x) to 2011.4s2 (CentOS 4.X) through ISO to 2011.4s2nsm2012.1_servers_upgrade_rs_5.7.zip

The purpose of this scenarios is to check if CentOS upgrade works for 2011.4s2. This scenario covers the following:

- Migration from 2009.1.r1a (SAM) build having 4.x CentOS version to 2011.4s2 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.

Scenario 3

2009.1r1a (CentOS 4.x) to 2010.3s4 (CentOS 4.x) through CentOS4.x_2012.1_server_upgrade.zip to 2012.1 (nsm2012.1_servers_upgrade_rs_5.7.zip)

The purpose of this scenarios is to migrate to 2012.1 with centos 4.x and ensure that Postgres is upgraded to 8.4.10. This scenario covers the following:

- Migration from 2009.1.r1a (SAM) build having 4.x CentOS version to 2010.3s4 build having CentOS 4.x.
- Migrated to 2012.1 using CentOS4.x_2012.1 zip files.

Scenario 4

2009.1r1a (CentOS 4.x) to 2011.4s2 (CentOS 4.x) through CentOS4.x_2012.1_server_upgrade.zip to 2012.1(nsm2012.1_servers_upgrade_rs_5.7.zip)

The purpose of this scenarios is to migrate to 2012.1 with centos 4.x and ensure that Postgres is upgraded to 8.4.10. This scenario covers the following:

- Migration from 2009.1r1a (SAM) build having 4.x CentOS version to 2011.4s2 build having CentOS 4.x.
- Migration to 2012.1 using CentOS4.x_2012.1 zip files.

Scenario 5

2009.1r1a (CentOS 4.x) to 2010.3s4 (CentOS 4.x) through CentOS4.x_2012.1_server_upgrade.zip to 2012.1(CentOS 4.x) through ISO to 2012.1 (nsm2012.1_servers_upgrade_rs_5.7.zip)

The purpose of this scenarios is to migrate 2012.1 from 2010.3 followed by Centos 5.7 upgrade. This scenario covers the following:

- Migration from 2009.1r1a (SAM) build having 4.x CentOS version to 2010.3s4 build having CentOS 4.x.
- Migration to 2012.1 using CentOS4.x_2012.1 zip files.
- Upgradation of CentOS to 5.7 using ISO.

Scenario 6

2009.1r1a (nsm2012.1_servers_upgrade_rs.zip) to 2011.4s2 (nsm2012.1_servers_upgrade_rs.zip) through CentOS4.x_2012.1_server_upgrade.zip to 2012.1(nsm2012.1_servers_upgrade_rs.zip) through ISO to 2012.1(nsm2012.1_servers_upgrade_rs_5.7.zip)

The purpose of this scenarios is to migrate 2012.1 from 2011.4 followed by Centos 5.7 upgrade. This scenario covers the following:

- Migration from 2009.1r1a (SAM) build having 4.x CentOS version to 2011.4s2 build having CentOS 4.x.
- Migration to 2012.1 using CentOS4.x_2012.1 zip files.
- Upgradation of CentOS to 5.7 using ISO.

Scenario 7

2009.1r1a (nsm2012.1_servers_upgrade_rs.zip) to 2010.3s4 (nsm2012.1_servers_upgrade_rs.zip) through ISO to 2010.3s4 (nsm2012.1_servers_upgrade_rs_5.7.zip) through CentOS 5.7_2012.1_server_upgrade.zip to 2012.1 (nsm2012.1_servers_upgrade_rs_5.7.zip)

The purpose of this scenarios is to upgrade to CentOS 5.7 followed by migration to 2012.1 from 2010.3 This scenario covers the following:

- Migration from 2009.1.r1a (SAM) build having 4.x CentOS version to 2010.3s4 build having CentOS 4.x . .
- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2012.1 using CentOS5.x_2012.1 zip files.

Scenario 8

2009.1r1a (nsm2012.1_servers_upgrade_rs.zip) to 2011.4s2 (nsm2012.1_servers_upgrade_rs.zip) through ISO to 2011.4s2 (nsm2012.1_servers_upgrade_rs_5.7.zip) through CentOS 5.7_2012.1_server_upgrade.zip to 2012.1(nsm2012.1_servers_upgrade_rs_5.7.zip)

The purpose of this scenarios is to upgrade to CentOS 5.7 followed by migration to 2012.1 from 2011.4. This scenario covers the following:

- Migration from 2009.1.r1a (SAM) build having 4.x centos version to 2011.4s2 build having centos 4.x . . .
- Upgradation of CentOS to 5.7 using ISO
- Migration to 2011.4s2.
- Migration to 2012.1 using centos5.x_2012.1 zip files.

Scenario 9

2009.1r1a (nsm2012.1_servers_upgrade_rs.zip) through ISO to 2010.3s1 (nsm2012.1_servers_upgrade_rs.zip) to 2010.3s1 (nsm2012.1_servers_upgrade_rs_5.7.zip) through Linux Build to 2010.3s4 (nsm2012.1_servers_upgrade_rs_5.7.zip) to 2011.4s (nsm2012.1_servers_upgrade_rs_5.7.zip) through CentOS 5.7_2012.1_server_upgrade.zip to 2011.4s2 (nsm2012.1_servers_upgrade_rs_5.7.zip) to 2012.1(nsm2012.1_servers_upgrade_rs_5.7.zip)

The purpose of this scenarios is to upgraded to CentOS 5.7 installation of different patches in 2010.3 and migration to 2011.4. and patches, using Linux build (as the zip files for these main and patch releases which are already published are with CentOS 4.x and old postgres support). This scenario covers the following:

- Migration from 2009.1.r1a (SAM) build having 4.x CentOS version to 2010.3s1 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.
- Refresh to 2010.3s1.
- Migration to 2010.3s4 using linux build.
- Migration to 2011.4s1 using linux build.
- Migration to 2011.4s2 using linux build
- Migration to 2012.1 using CentOS4.x_2012.1 zip files.

Scenario 10

2009.1r1a (nsm2012.1_servers_upgrade_rs.zip) to 2011.4s1 (nsm2012.1_servers_upgrade_rs.zip) through CentOS 5.7_2012.1_server_upgrade.zip to 2011.4s2 (nsm2012.1_servers_upgrade_rs_5.7.zip) to 2012.1(nsm2012.1_servers_upgrade_rs.zip) through ISO to 2012.1(nsm2012.1_servers_upgrade_rs_5.7.zip)

The purpose of this scenarios is check CentOS upgrade after upgrade to 2012.1 from 2011.4 s1. This scenario covers the following:

- Migration from 2009.1.r1a (SAM) build having 4.x CentOS version to 2011.4s1 build having CentOS 4.x.
- Migration to 2012.1 using CentOS4.x_2012.1 zip files.
- Upgradation of CentOS to 5.7 using ISO

CHAPTER 8

Maintaining NSM

This chapter describes basic procedures used to administer Network and Security Manager (NSM). These procedures include instructions describing how to manually send commands to the management system such as start and stop, configure the GUI server, Device server and HA server manually, configure the local database backup option, install a TFTP server (required if you are managing security devices running ScreenOS 5.0.x), and uninstall the management system and User Interface.

This chapter contains the following sections:

- [Controlling the Management System on page 251](#)
- [Configuring Server Options on page 254](#)
- [Archiving and Restoring Logs and Configuration Data on page 258](#)
- [Configuring High Availability Options on page 260](#)
- [Relocating the Database on page 263](#)
- [Installing a Trivial File Transfer Protocol Server on page 267](#)
- [Modifying Timeout Values on the Device Server on page 268](#)
- [Downgrade Procedures on page 269](#)
- [Removing the Management System on page 270](#)
- [Uninstalling the User Interface on page 271](#)

Controlling the Management System

On occasion, it may become necessary to start or stop the management system processes manually. You can control the management system by navigating to the appropriate “bin” subdirectory for the Device server, GUI server, or HA server, and then issuing a manual command.

Viewing Management System Commands

To view the manual commands that you can send to the GUI server:

1. Navigate to the GUI server bin subdirectory. For example:

```
cd /usr/netscreen/GuiSvr/bin
```

2. Run the following command:

```
./guiSvr.sh
```

To view the manual commands that you can send to the Device server:

1. Navigate to the Device server bin subdirectory. For example:

```
cd /usr/netscreen/DevSvr/bin
```

2. Run the following command:

```
./devSvr.sh
```

To view the manual commands that you can send to the HA server:

1. Navigate to the HA Server bin subdirectory. For example:

```
cd /usr/netscreen/HaSvr/bin
```

2. Run the following command:

```
./haSvr.sh
```

Common Management System Commands

Table 23 on page 252 describes the commands that the management system supports.

Table 23: Management System Commands

Command	Action
reload	Sends a hangup signal to the management system process, and then instructs the process to reload its configuration and start again.
restart	Stops the management system process for two seconds, and then restarts the process.
start	Starts the management system process.
stop	Stops the management system process.
status	Provides a status of the management system process.
version	Lists the current version of the management system.

Starting All Server Processes Using the HA Server

If you have installed the HA Server process, we recommend that you start all the management server processes by simply starting the HA Server process.

To start the HA Server process manually, enter the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

The HA Server process automatically starts the GUI server and Device server processes.

NSM server processes always run with nsm user permissions, even if you have root user permissions when you start them.

Starting GUI Server and Device Server Processes Manually

If you have not installed the HA server process, you can manually start the GUI server and Device server processes.

To start the GUI server manually, enter the following command:

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh start
```

To start the Device server manually, enter the following command:

```
/usr/netscreen/DevSvr/bin/devSvr.sh start
```

NSM server processes always run with nsm user permissions, even if you have root user permissions when you start them.

Stopping Server Processes

You can manually stop each server process as follows.

To stop the GUI server manually, enter the following command:

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop
```

To stop the Device server manually, enter the following command:

```
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

To stop the HA Server process manually, enter the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop
```



NOTE: To prevent the server from rebooting in a HA configuration that uses shared disks, you must ensure that none of the shared files are in use before stopping the HA server process. If these files are in use (for example, by a vi or tail command), then the configured file system unmount command will fail, causing the server to reboot.

Configuring Server Options

The following procedures are provided for your reference:

- [Changing the Management System IP Address on page 254](#)
- [Changing the Device Server IP Address on page 255](#)
- [Changing the GUI Server IP Address on page 255](#)
- [Configuring Disk Space Management on the Device Server on page 255](#)
- [Configuring Disk Space Management on the GUI Server on page 256](#)
- [Configuring Connection Timing on page 257](#)
- [Setting Core File Naming on Solaris on page 258](#)

Changing the Management System IP Address

If you have installed the management system on a single server (in the standalone configuration), and you move it later to a different server, then you need to reconfigure the management IP address and port, enabling your managed devices to connect to it at its new location.

To change the management system IP address:

1. Update the Device server IP on each managed device or set the secondary management server IP to the new IP address.
2. Log into the new NSM server as root.
3. Navigate to `/usr/netscreen/DevSvr/var`.
4. Open the Device server configuration file (`devSvr.cfg`) in any text editor.
5. Edit the values for the `guiSvr.addr` and `guiSvr.port` variables using the new IP address and port number.
6. Save the Device server configuration file.
7. Navigate to the `utils` directory. Run the `.xdbUpdate` utility to update the IP Address. Run the following:

```
export LD_LIBRARY_PATH=/usr/netscreen/GuiSvr/utils/dbxm1-2.2.13/lib
cd /usr/netscreen/GuiSvr/utils
./xdbUpdate /usr/netscreen/GuiSvr/var/xdb server 0 0 /_/ip <IP Address>
./xdbUpdate /usr/netscreen/GuiSvr/var/xdb server 0 1 /_/ip <IP Address>
```

Note that the 0 represents the GUI server ID and the 1 represents the Device server. You can view these IDs using the Server Manager in the NSM UI.

8. Restart the GUI server, and then restart the Device server.

Changing the Device Server IP Address

If you have installed the management system on separate servers (in the distributed configuration), and you later move the Device server to a different server, you need to reconfigure the management IP address and port enabling your managed devices to connect to it at its new location. To do this, use the `.xdbUpdate` utility on the GUI server.

To change the Device server IP Address:

1. Log into the server that is running the GUI server as root. Navigate to the `utils` directory. Run the `.xdbUpdate` utility to update the IP Address. Run the following:

```
export LD_LIBRARY_PATH=/usr/netscreen/GuiSvr/utils/dbxm1-2.2.13/lib
cd /usr/netscreen/GuiSvr/utils
./xdbUpdate /usr/netscreen/GuiSvr/var/xdb server 0 1/___/ip <IP Address>
```

Note that the 1 represents the Device server. You can view this ID using the Server Manager in the NSM UI.

2. Restart the GUI server.

Changing the GUI Server IP Address

If you have installed the management system on separate servers (in the distributed configuration), and you later move the GUI server to a different server, then you need to reconfigure the management IP address and port enabling the Device server to connect to it at its new location. To do this, use the `.xdbUpdate` utility on the GUI server.

To change the GUI server IP address:

1. Login to the GUI server. Navigate to the `utils` directory.
2. Run the following:

```
export LD_LIBRARY_PATH=/usr/netscreen/GuiSvr/utils/dbxm1-2.2.13/lib
cd /usr/netscreen/GuiSvr/utils
./xdbUpdate /usr/netscreen/GuiSvr/var/xdb server 0 0/___/ip <IP Address>
```

3. Restart the GUI server.

Configuring Disk Space Management on the Device Server

By default, the Device server maintains a minimum of 1000 MB of disk space, primarily for the storage of log records. When the available disk space reaches this minimum, the Device server sends an e-mail alerting you of the situation. In the event that disk space on the Device server reaches a minimum of 500 MB, the Device server attempts to free the disk space by purging log records beginning with the oldest records on file. The Device server stops purging log records when the 1000 MB minimum disk space is restored. If for any reason, the Device server is not able to restore 500 MB of disk space, the Device server automatically shuts down. An error message appears in the console window

indicating that there is not enough disk space on the server machine, and that you must either backup your data or free up additional disk space in order to start the server again.

To change the parameters for managing disk space on the Device server, edit the Device server configuration file.

To configure disk space management:

1. Log into the server that is running the Device server as root.
2. Navigate to **`usr/netscreen/DevSvr/var`**.
3. Open the Device server configuration file (called **`devSvr.cfg`**) in any text editor.
4. Edit the value (in megabytes) for the `storageManager.threshold` parameter. This parameter sets the minimum threshold at which the Device server begins purging log records. The Device server purges log records when disk space reaches 800 MB by default.
5. Edit the value (in megabytes) for the `storageManager.minimumFreeSpace` parameter. This parameter indicates that 1000 MB of disk space need to be free if the Device server starts to purge log records after crossing `storageManager.threshold`.
6. Edit the value (in megabytes) for the `storageManager.alert` parameter. This parameter sets the minimum threshold for available disk space at which the Device server sends you an e-mail alert. By default, the Device server sends an e-mail alert when disk space reaches 1500 MB.



NOTE: Use the Server Manager node in the UI to configure e-mail notification. Refer to the *Network and Security Manager Administration Guide* for more information.

7. Save the file.
8. Restart the Device server.

Configuring Disk Space Management on the GUI Server

Disk space management occurs in the same manner on the GUI server except that there is no log record purging on the GUI server side. When the GUI server reaches the minimum disk space threshold, it automatically shuts down. You will not be able to restart the GUI server until you restore the minimum disk space.

The GUI server also performs a checks for sufficient i-nodes. I-nodes are data structures that contain information about files in a Unix file system. Each file has an inode that is identified by an inode number (i-number) in the file system where it resides. There are a set number of inodes, which indicates the maximum number of files the system can hold. If the required minimum i-nodes is not available, the GUI server shuts down automatically. The default threshold is 10 percent of the total i-nodes remaining. You will not be able to restart the GUI server until you reclaim required minimum i-nodes. For your convenience, a shell script is provided enabling you to reclaim i-nodes. This script is located in the utilities directory on the GUI server (**`/usr/netscreen/GuiSvr/util`**). The script first archives

the old domain versions into a compressed tar file before removing them to reclaim i-nodes. The archive file is stored in:

```
/usr/netscreen/GuiSvr/var/global/oldDomainVersion.MM-DD-YYYY-HH-MM.tar.gz
```

You can configure disk space management on the GUI server edit the GUI server configuration file (called `guiSvr.cfg`).

To configure disk space management:

1. Log into the server that is running the GUI server as root.
2. Navigate to `usr/netscreen/GuiSvr/var`.
3. Open the GUI server configuration file (called `guiSvr.cfg`) in any text editor.
4. Edit the value (in megabytes) for the `storageManager.threshold` parameter. This parameter sets the minimum threshold at which the GUI server begins purging log records. The GUI server purges log records when disk space reaches 500 MB by default.

If you are running the Device server and GUI server on the same machine, we recommend that you set the `storageManager.threshold` on the Device server to a value that is higher than that on the GUI server. By doing this, the GUI server will not shut down as the Device server attempts to free up some disk space by purging logs.

5. Edit the value (in megabytes) for the `storageManager.minimumFreeSpace` parameter. This parameter indicates that 1000 MB of disk space need to be free if the GUI server starts to purge log records after crossing `storageManager.threshold`.
6. Edit the value (in megabytes) for the `storageManager.alert` parameter. This parameter sets the minimum threshold for available disk space at which the GUI server sends you an e-mail alert. By default, the GUI server sends an e-mail alert when disk space reaches 1000 MB.



NOTE: Use the Server Manager node in the UI to configure e-mail notification. Refer to the *Network and Security Manager Administration Guide* for more information.

7. Configure the minimum i-node threshold by editing the `storageManager.inodeThres` variable.
8. Save the file.
9. Restart the GUI server.

Configuring Connection Timing

To configure connection timing with the managed devices in your network:

1. Edit the Device server configuration file (called `devSvr.cfg`).
2. Edit the time value (in thousandths of a second) for the `devSvrDirectiveHandler.fastCli.timeout` parameter to change the way the Device

server controls connection timing with managed security devices running ScreenOS. The `devSvrDirectiveHandler.fastCli.timeout` parameter determines the amount of time that the Device server waits for a CLI response from a security device running ScreenOS before it disconnects the connection. By default, the Device server waits 40 seconds before disconnecting the connection.

3. Save the file.
4. Restart the Device server.

Setting Core File Naming on Solaris

If you are running the management system on Solaris, you can configure the file naming used for core files to indicate the executable file and process ID generating the core file. This procedure also ensures that Solaris does not overwrite the names of multiple core files.

To set core file naming on Solaris:

1. Log into the GUI server as root.
2. Run the following command:

```
coreadm -i core.%f.%p
```

3. Restart the server.

Future core files will indicate the executable filename and process ID generating the core file. For example, if the core file **core.a.out.8855** appears, the filename indicates that the core file was generated by an executable named **a.out**, running process ID 8855.

Archiving and Restoring Logs and Configuration Data

You can archive and retrieve configuration and log data in NSM using standard UNIX commands. All your configuration information, including device configuration data, administrators, policies, audit logs, and job information is stored on the GUI server. Logs reside on the Device server.

Archiving Logs and Configuration data

Before you begin archiving, it is important that you first stop the processes running on both servers. After you have stopped both servers, you will then need to identify the actual location of the GUI server and Device server data directories. These are the directories that you need to back up. You can do this by running an “ls -al” command on the following directory locations:

- **/usr/netscreen/GuiSvr/var** (or the path that you configured when you initially installed the GUI server)
- **/usr/netscreen/DevSvr/var** (or the path that you configured when you initially installed the Device server)

To archive log and configuration data:

1. Stop the HA Server; stop the Device server; and then stop the GUI server.
2. Use the **ls -al** command to discover the actual paths of the GUI server and Device server data directories.

```
is -al /usr/netscreen/GuiSvr/var
```

```
lrwxrwxrwx 1 root root 21 Apr 11 15:04 /usr/netscreen/GuiSvr/var ->
/var/netscreen/GuiSvr
```

This output indicates that the actual location of the GUI server data is in **/var/netscreen/GuiSvr**.

Verify where your data is stored and which directories should be backed up on your own system. Follow the same procedure to determine the location of your data on the Device server.

```
is -al /usr/netscreen/DevSvr/var
```

```
lrwxrwxrwx 1 root root 21 Apr 11 15:02 /usr/netscreen/DevSvr/var ->
/var/netscreen/DevSvr
```

3. Run the appropriate backup command on your Solaris or Linux platform to backup the GUI server data. For example:

```
tar -cvf /netscreen_backup/db-data.tar /var/netscreen/GuiSvr
gzip db-data.tar
```

4. Run the appropriate backup command on your Solaris or Linux platform to backup the Device server data. We recommend that you use either Secure Copy or FTP to the Device server data.



NOTE: Using tar may not be appropriate for log data in the Device server which may be large.

For example, you can use scp by running the following command:

```
scp -r <local directory> usr@host:<remote-directory>
```

For example, you can use ftp by running the following commands:

```
ftp <host name>
bi
hash
lcd <local directory>
prompt
mput
```

5. We recommend that you relocate backup copies of both the GUI server configuration data and Device server log data to an external location or disk.
6. Start the HA Server, GUI server, and then the Device server.



NOTE: Do not start the GUI server and the Device server manually if the HA Server will start them for you. The HA Server starts these processes automatically:

- in HA configurations.
- in non-HA configurations in which you chose during installation to have processes restarted automatically in case of failure.

Restoring Logs and Configuration Data

To restore log and configuration data:

1. Stop the HA Server, Device server, and then the GUI server.
2. Use the **mv** command to move data from the “var” directories (for example, `/var/netscreen/GuiSrv` and `/var/netscreen/DevSrv`) to a safe location.
3. Untar or place your backups into the var directories.
4. Start the HA Server, GUI server, and then the Device server.



NOTE: Do not start the GUI server and the Device server manually if the HA Server will start them for you. The HA Server starts these processes automatically:

- in HA configurations.
- in non-HA configurations in which you chose during installation to have processes restarted automatically in case of failure.



NOTE: These instructions apply only to systems where the “var” links point to a true location outside the prescribed locations (`/usr/netscreen/GuiSrv` or `/usr/netscreen/DevSrv`). It is not recommend that you have these links point to locations that are inside `/usr/netscreen/GuiSrv` or `/usr/netscreen/DevSrv`. Doing so complicates any upgrade of NSM and requires special precautions during backup and restore.

Configuring High Availability Options

You can manually configure the high availability options on the management system by editing the High Availability configuration file (`haSrv.cfg`).

Enabling and Disabling High Availability Processes

To enable high availability:

1. Stop the HA Server, Device server, and then the GUI server.
2. Navigate to the High Availability configuration directory. For example:

```
cd /usr/netscreen/HaSvr/var/
```

3. Open the High Availability configuration file (**haSvr.cfg**) in any text editor.
4. To enable high availability, configure the following parameters:

```
highAvail.isHaEnabled=y
highAvail.isWatchdogEnabled=n
```

5. Save the file.
6. Restart the HA Server process. To do this, you must send a HUP signal to the highAvail process. For example:

```
kill -HUP <process id>
```

Use the **haStatus** command to identify the highAvail process ID.

Sending a HUP signal to the highAvail process restarts the HA Server process. You do not need to restart the server manually.

To disable high availability, follow the above procedure, configure the following parameter in the **haSvr.cfg** file, save the file, and restart the HA Server:

```
highAvail.isHaEnabled=n
```

Configuring Other High Availability Options

Other parameters in the High Availability configuration file enable you to change how high availability works in your network.

To configure other high availability options:

1. Stop the running server processes.
2. Navigate to the HA Server configuration directory (**var/netscreen/HaSvr** by default).
3. Open the HA Server configuration file (**haSvr.cfg**) in any text editor.
4. Configure the file as needed:
 - To change the HA Server (and local database) backup directory, edit the value for the **highAvail.pathDbBackup** variable.
 - To change the time of day that the HA replication begins, edit the value for the **highAvail.backupTimeHour** variable.

- To change the number of backup files that the tool saves, edit the value for the `highAvail.numofBackup` variable.
 - To change the path to the rsync package, edit the value for the `highAvail.rsyncLocation` variable.
 - To change the heartbeat interval, edit the value for the `highAvail.heartbeatInterval` variable.
5. Save the file.
 6. Restart the HA Server process. To do this, you must send a HUP signal to the `highAvail` process. For example:

```
kill -HUP <process id>
```



NOTE: Use the `haStatus` command to identify the `highAvail` process ID.

Backing Up the Database Locally

A shell archive script is provided to manually backup the database locally.

To replicate the database locally:

1. Stop the running server processes.
2. Navigate to the HA Server utilities subdirectory (`/usr/netscreen/HaSvr/utls` by default).
3. Run the replicate database shell archive script. You can do so by running the following command as `nsm` user:

```
./replicateDb backup
```

Or you can run the following command as root user:

```
su nsm ./replicateDb backup
```

The local backup is created in the directory specified by the `highAvail.pathDbBackup` parameter in the High Availability configuration file. By default, it is created in `/var/netscreen/dbbackup`.

Restoring the Database

If you need to restore the database, you can use a shell archive script.

To restore the database:

1. Install NSM on a new server machine. The new server machine is required to use:
 - the same IP Address as the previous server on which you ran the GUI server
 - the same operating system that you ran on the previous server

During the installation, you must also install and configure the local database backup option on both the GUI server and Device server.

2. Save your remote copy of the database backup files for the appropriate day of the week to the local database backup data directory on your new management system server.
3. Navigate to the HA Server utilities subdirectory (`/usr/netscreen/HaSvr/utls` by default).
4. Run the database restore shell archive script and specify the number day of the week for the backup file that you want to restore from (N = backup day of the week). For example:

```
restoreDbFromBackup.sh N
```

For example, to restore the backup file from Friday:

```
sh restoreDbFromBackup.sh 5
```

The restore script:

1. Prompts you to confirm stopping the running server process(es).
2. Verifies that you have properly logged in as the root user.
3. Verifies that the backup file specified exists.
4. Stops all running server processes.
5. Uses rsync to copy the backup file to the appropriate server directories.
6. Restarts all server processes.

Validating the Database Recovery Process

If you are using the local database backup option on a network where the GUI server and Device server are installed on separate systems and you did not install the local database backup option properly on the GUI and Device Servers, then devices might not reconnect to the management system after you have restored the database. In this event, contact technical support for assistance.

Changing the HA Server IP Address

If for any reason you are required to change the IP address of either the primary or secondary HA Server, you must manually reimport or update the IP Address on the device.

Relocating the Database

To move the database from one system to another, follow these steps:

1. Archive the database on the GUI server.
2. Archive the log database on the Device server.
3. Install NSM on a new system.
4. Copy over the GUI server database on the new system.
5. Copy over the Device server log database on the new system.

Archiving the GUI Server Database and Device Server Log Database

To archive the GUI server database and the Device server log database:

1. Verify that the system is working properly.
2. Stop the server processes:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop
```

If the HA Server is not configured to stop the GUI server and the Device server automatically, stop the GUI server, and then stop the Device server:

```
/usr/netscreen/DevSvr/bin/devSvr.sh stop  
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop
```

3. Tar and compress the current GUI server database. You can do so by running the following commands:

```
tar -cvf guidb.tar /var/netscreen/GuiSvr  
gzip guidb.tar
```

4. Verify that you have sufficient disk space available on the Device server to backup your current logs.
5. Tar and compress the current Device server logs. You can do so by running the following commands:

```
tar -cvf devsvrdb.tar /var/netscreen/DevSvr/logs  
gzip devsvrdb.tar
```

Installing NSM On a New System

See [“Installing NSM in a Standalone Configuration” on page 15](#) for more information on installing NSM on the same server machine.

See [“Installing NSM in a Distributed Configuration” on page 49](#) for more information on installing NSM on separate server machines.

Moving the Databases to the New System

Move the GUI server database to the new system:

1. Stop the GUI server.
2. Backup all the files (using tar) located in `/var/netscreen/GuiSvr` on your current system.
3. Perform a clean install of the GUI server on the new system.
4. Copy the tar file from your current system to the new system.
5. Remove all files in the GUI server var directory. For example:

```
rm -rf /var/netscreen/GuiSvr
```

6. Untar the GUI server backup files.
7. Navigate to the utils directory. Run the `.xdbUpdate` utility to update the IP Address. For example, you would run the following commands:

```
cd /usr/netscreen/GuiSvr/utils
./xdbUpdate.sh /usr/netscreen/GuiSvr/var/xdb server 0 0 /__ip 10.1.1.2
./xdbUpdate.sh /usr/netscreen/GuiSvr/var/xdb server 0 1 /__ip 10.1.1.2
```

Note that the 0 represents the GUI server ID and the 1 represents the Device server. You can view these IDs using the Server Manager in the NSM UI.

Copy the Device server log database to the new system:

1. On the Device server, unzip and untar the old Device server logs database. You can either recursive copy the files or replace the new database with the old one.
2. Navigate to the `/var/netscreen/DevSvr/logs` directory and delete all the `.mark` files. You can do so by running the following commands:

```
rm -rf *.mark
```

Reset the RSA keys between GUI server and Device server:



CAUTION: Resetting RSA keys involves editing your database. Editing errors could corrupt your data. The commands you use are the same as those in a vi editor. If you are not familiar with vi, seek assistance.

1. Run `xdbViewEdit` using the command: `/usr/netscreen/GuiSvr/utils/xdbViewEdit.sh`
 - a. Set the path of vi editor to `/bin/vi` if prompted.
 - b. Open in read-write mode.
 - c. Select `<0.shadow_server.1>` (option 7).
 - d. View and make note of the client one-time password in the `shadow_server` table.
 - e. Delete the devSvr RSA keys.

```
:ourRsaPrivateKey
(0010EF1E322A3D14ABAFF5CB9DF5BF5870070010F863D39A18637
8507CCD5E0E18308F270020E8027 EEC23CC60D454B01A75642FE28
DCA4B165E808DD90FE0D933CA3

65CFA110001250020 E1BD3D38C8E287B9D5DBC6B76865
F12E28C3A1736830CBD7A98A9721DFB97E7

:theirRsaPublicKey
(0020CBCE9B75418130C8805A3EDD7E21C6775FEAFCD92155F0E2
101EA2A4B06F0B25000125)
```

f. Save and exit from the **O.shadow_server.1** table

g. Select option 12 to save and exit from `xdbViewEdit`.

2. Edit `/usr/netscreen/DevSvr/var/devSvr.cfg`

- a. Delete the `ourRsaPrivateKey` and `theirRsaPublicKey` lines in **devSvr.cfg**. Remove them entirely.
- b. Change the one-time password in **devSvr.cfg** to match the one-time password in the **O.shadow_server.1** table if necessary.
- c. Verify that the `GuiSvr` IP addresses are correct.
- d. Save the file and exit.

Restart the server processes:

1. Start the HA Server:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

2. If the HA Server is not configured to start the GUI server and the Device server automatically, start the GUI server, and then start the Device server:

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh start
/usr/netscreen/DevSvr/bin/devSvr.sh start
```

3. Verify that all the server processes are running:

```
/usr/netscreen/HaSvr/bin/haSvr.sh status
/usr/netscreen/GuiSvr/bin/guiSvr.sh status
/usr/netscreen/DevSvr/bin/devSvr.sh status
```

Installing a Trivial File Transfer Protocol Server

If you are using NSM to manage security devices running ScreenOS 5.0.x, then you need to install and run a Trivial File Transfer Protocol (TFTP) server on the system that is running the Device server. The TFTP server is required to enable certificate management for security devices running ScreenOS versions 5.0.x.

Installing a TFTP Server on Linux

Before installing the TFTP server on your Red Hat Linux server, check for previous installations.

To verify if the TFTP server is already installed on your Linux server, run the following command:

```
rpm -q tftp-server
```

If the TFTP server is installed, the output indicates the following:

```
tftp-server-<version>-<revision>
```

For example, the output for an unpatched Red Hat 9.0 server is as follows:

```
tftp-server-0.32-4
```

If the TFTP server is not installed, then download and install the package from the Red Hat Linux installation CD or from the Internet at the Red Hat or Red Hat mirror site. After the package is installed, you must enable and configure the TFTP server.

To configure and enable the TFTP server on Linux:

1. Open the `/etc/xinetd.d/tftp` file in any text editor.
2. Edit the parameter “server_args =” so that the value is “-s /usr/netscreen/DevSvr/var/cache”.
3. Edit the parameter “disable” so that the value is “no”. The file should now appear as follows:

```
service tftp
socket_type = dgram
protocol = udp
wait = yes
user = root
server = /usr/sbin/in.tftpd
server_args = -s /usr/netscreen/DevSvr/var/cache
disable = no
per_source = 11
cps = 100 2
}
```

- Restart the xinetd service. For example:

```
service xinetd restart
```

Installing a TFTP Server on Solaris

By default, Solaris installs the TFTP service on your machine but leaves it disabled.

To configure and enable the TFTP service on Solaris:

- Open the `/etc/inetd.conf` file in any text editor.
- Uncomment the line that begins with “tftp” or “#tftp” .
- Edit the same line by replacing “in.tftpd -s /tftpboot” at the end of the line with “in.tftpd -s /usr/netscreen/DevSvr/var/cache” . The line should now appear as follows:

```
tftp dgram udp wait root /usr/sbin/in.tftpd
in.tftpd -s /usr/netscreen/DevSvr/var/cache
```

- Restart the inetd service. You can do so by running the following commands:

```
/etc/init.d/inetd stop
/etc/init.d/inetd start
```

Modifying Timeout Values on the Device Server

On occasion, it may become necessary to modify certain timeout values on the Device server, for example if you receive errors when sending bulk command line interface (CLI) commands or updating certain security systems. You can modify these timeout values by editing a configuration file on the Device server called `devCommProp.cfg`.

To modify timeout values on the Device server:

- Stop the Device server and any HA server:
 - If the HA server is configured to stop all NSM server processes when it stops, enter this command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop
```

- If the HA Server is not configured to stop all NSM server processes when it stops, enter these commands:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

- Open the following file in a text editor:

```
/var/netscreen/DevSvr/be/cfg/devCommProp.cfg
```

3. Locate the following line:

```
:bulk-cli-final-status-timeout (40)
```

4. Change the “40” to a value from 1 to 39.
5. Locate the following line:

```
:pooh-timeout
```

6. Change the “10” to a value 20 (minutes).
7. Save the file.
8. Start the HA Server process:

```
/usr/netscreen/HaSvr/bin/haSvr.sh start
```

9. If HA Server process is not configured to start the GUI server and the Device server when it starts, start the GUI server, and then start the Device server:

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh start
/usr/netscreen/DevSvr/bin/devSvr.sh start
```

10. Verify that the server processes are running:

```
/usr/netscreen/HaSvr/bin/haSvr.sh status
/usr/netscreen/GuiSvr/bin/guiSvr.sh status
/usr/netscreen/DevSvr/bin/devSvr.sh status
```

Downgrade Procedures

To downgrade to your previous version of NSM, you need to reinstall that version of NSM, and restore your old data.



NOTE: Before downgrading, check the audit log for any changes made since the upgrade that you might need to restore once the downgrade is complete.

To downgrade from NSM:

1. Make a backup copy of all your existing data.
2. Remove the management system. See [“Removing the Management System” on page 270](#) for more information.

3. Install your previous version of NSM.
4. Restore your backup database. See ["Restoring the Database" on page 262](#) for more information.

Removing the Management System

To remove previous management system installations:

1. Stop the HA Server by entering the following command:

```
/usr/netscreen/HaSvr/bin/haSvr.sh stop
```

2. Stop the Device server by entering the following command:

```
/usr/netscreen/DevSvr/bin/devSvr.sh stop
```

3. Stop the GUI server by entering the following commands:

```
/usr/netscreen/GuiSvr/bin/guiSvr.sh stop
```

4. For systems running Linux:

- a. Navigate to the `/usr` subdirectory, and remove all the files in the `netscreen` subdirectory.

```
rpm -e netscreen-DevSvr  
rpm -e netscreen-GuiSvr  
rpm -e netscreen-HaSvr  
rm -rf netscreen
```

- b. Navigate to the `/var` subdirectory, and remove all the files in the `netscreen` subdirectory.

```
rm -rf netscreen
```

5. For systems running Solaris:

- a. Locate and remove all packages related to NSM in the `netscreen` subdirectory. For example, run the following commands:

```
pkginfo | grep -i netscreen  
application NSCNhasv Network and Security Manager HA Server  
application NSCNguisv Network and Security Manager GUI Server  
application NSCNdevsv Network and Security Manager Device Server  
root# pkgrm -R / NSCNdevsv  
The following package is currently installed:  
NSCNdevsv Network and Security Manager Device Server  
(sparc) 1.3.2  
Do you want to remove this package? [y,n,?,q] y  
## Removing installed package instance <NSCNdevsv> ## Verifying package  
dependencies.  
## Processing package information.
```

```
## Removing pathnames in class <none>
/usr/netscreen/DevSvr/utils/policy_compiler
/usr/netscreen/DevSvr/utils/nacnUpdateCANml
/usr/netscreen/DevSvr/utils/nacnLoadPKCS12
...
/usr/netscreen/DevSvr/bin/.devSvrDataCollector
/usr/netscreen/DevSvr/bin
/usr/netscreen/DevSvr <non-empty directory not removed> ## Updating system
information.
Removal of <NSCNdevsv> was successful.
```

- b. Repeat this step for each package.
- c. Remove the netscreen subdirectory.
- d. Remove the startup script links. For example, run the following commands:

```
cd /etc/rc3.d
/etc/rc3.d root# ls *Svr
S32haSvr S33guiSvr S34devSvr
/etc/rc3.d root# rm -f *Svr
/etc/rc3.d root#
```

- e. Remove the actual scripts. For example, run the following commands:

```
cd ../init.d
etc/init.d root# ls *Svr
devSvr guiSvr haSvr
etc/init.d root# rm -f *Svr
etc/init.d root#
```

6. Remove the nsm user and group:

```
userdel nsm
groupdel nsm
```

Uninstalling the User Interface

If you need to uninstall the NSM UI, run the NSM uninstall program.



NOTE: If you are uninstalling the UI on a Windows-based , it is not recommended that you use the Add/Remove Programs utility to remove the NSM UI.

To uninstall the NSM UI:

1. On a Windows-based , use the Start menu, then select **Network and Security Manager>Uninstall Network and Security Manager**.

On a Linux-based , you can either double-click on the **Uninstall_Network_and_Security Manager** icon, or you can launch the UI uninstaller from a command line.

```
sh Uninstall_Network_and_Security_Manager
```

The uninstaller launches.

2. Click the **Uninstall** button to uninstall the UI. The uninstaller proceeds to uninstall all the UI software files, shortcuts, folders, and registry entries.

When the uninstaller has finished, a window appears indicating that all files were successfully uninstalled.

3. Click **Done** to exit the uninstaller.

PART 2

Appendixes

- [Technical Overview of the NSM Architecture on page 275](#)
- [Hardware Recommendations on page 283](#)
- [Profiler Performance Tuning Recommendations on page 291](#)

APPENDIX A

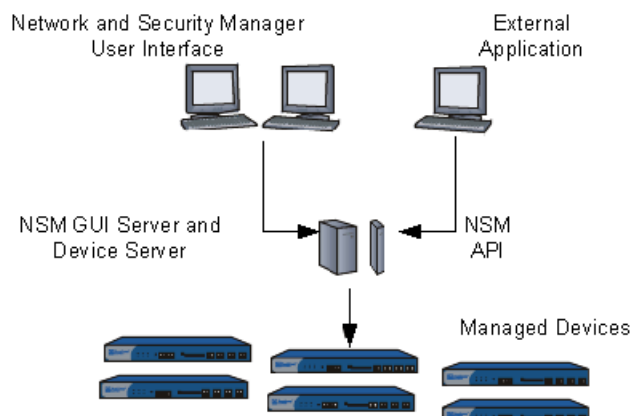
Technical Overview of the NSM Architecture

This appendix describes the Network and Security Manager (NSM) three-tiered architecture.

The NSM management architecture is designed to provide optimum security, scalability, and flexibility for integrating with your specific network security environment. It includes the following key components as shown in [Figure 15 on page 275](#):

- Management system
- User interface (UI)
- Managed devices

Figure 15: NSM Architecture



This appendix contains the following sections:

- [About the Management System on page 276](#)
- [About the NSM User Interface on page 277](#)
- [About Managed Devices on page 277](#)
- [Server Communications on page 277](#)
- [Using the Secure Server Protocol on page 279](#)

- [Communications with Devices Running ScreenOS 5.X and Later on page 280](#)
- [Communications with Device Management Interface-Compatible Devices on page 281](#)
- [Creating a Separate Management Network on page 281](#)

About the Management System

The management system itself is made up of these components:

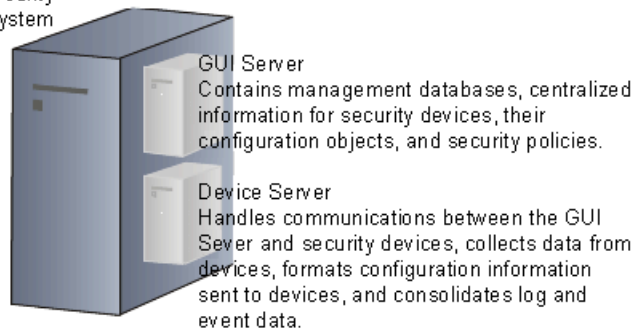
- GUI server
- Device server
- HA server

The GUI server and Device server working together are collectively referred to as the NSM management system.

[Figure 16 on page 276](#) shows these components.

Figure 16: NSM Management System

Network and Security
Management System



You can install both components of the management system on the same physical server or on separate servers. By separating the two server components, you can improve system performance.

GUI Server

The GUI server receives and responds to requests and commands from the NSM UI. It manages all the system resources and configuration data required to manage your network. It also contains a local data store including all device configuration information, audit log data (versioning), and almost all other information pertinent to the system except log data sent by the managed device.



NOTE: The GUI server can accommodate no more than 10 UI clients connected to it when NSM manages 3000 low-end devices, and no more than 25 UI clients connected to it when NSM manages 300 high-end devices. This limit is the maximum number of UI clients supported in this release of NSM.

Device Server

The Device server acts as a collection point for all data generated by the managed devices in your network. The Device server stores this data, primarily traffic logs generated by a managed device, in a local data store.



NOTE: The Device server can accommodate no more than 3000 low-end managed devices or 300 high-end managed devices connected to it at any time. This limit is the maximum number of managed devices supported in this release of NSM.

HA Server

An additional server process, called the HA Server, continuously monitors the GUI server and Device server processes. If the HA Server process detects that either the GUI server or Device server is down, then it automatically restarts the process.

About the NSM User Interface

The NSM User Interface (UI) is a Java-based software application that you use to access and configure data about your network on the management system. After you have installed the UI, you can launch it and connect it to the management system. From the UI, you can view, configure, and manage your network from a single, central administrative location. Refer to the *Network and Security Manager Administration Guide* or the *Network and Security Manager Online Help* included in the UI for more information about the NSM UI.

About Managed Devices

The managed devices that you have implemented in your network are the lowest tier of the NSM management architecture.

You need to enable each managed device to communicate and work with NSM. See the manual appropriate to the specific device family for more information describing how to enable management on your devices.

Once enabled, each managed device communicates and sends information to the NSM management system. From NSM, you can centralize all configuration data and manage the network from a single, central, administrative location. You can then implement your security policies by “pushing” or sending configuration updates back to your devices.

Based on the device configuration and security policies you define in NSM, the managed devices provide the firewall and VPN services required to secure your network environment.

Server Communications

As you plan your installation, it helps to understand how NSM establishes communication among the UI, Management System, and managed devices.

Communication Ports and Protocols

For optimum security, the total number of open ports on the GUI server and Device server is kept to a minimum. For best practices on mitigating the vulnerabilities of open ports in UNIX on which NSM is built and deployed, refer

<http://www.juniper.net/us/en/local/pdf/app-notes/3500183-en.pdf>.

The following tables list the inbound and outbound ports on the NSM management system.

Table 24: Inbound ports on the NSM Management System

Port	Protocol	Description
22	TCP	In an HA setup, the HA server synchronizes the Primary and Secondary NSM servers using rsync to transfer files through this port.
443	TCP	The client accesses the NSMXpress Web interface using this port.
5432	TCP	STRM devices connect to the PostgreSQL on this port to get profiler data.
7800	TCP	Devices running ScreenOS Software connect to the Device server on this port.
7801	TCP	<ul style="list-style-type: none"> The GUI server receives communication from the Device server on this port In releases earlier than NSM 2008.2, the GUI client connects to the GUI server on this port.
7802	UDP	In an HA installation, heartbeats are sent to the peer on this port.
7803	TCP	IDP Series sensors connect with the Device server on this port.
7804	TCP	Devices running Junos OS, IC Series, SA Series, and EX Series devices connect with the Device server on this port.
7808	TCP	From release 2008.2 onwards, the GUI client connects with the GUI server on this port.
8443	TCP	Optional; this port is used to download the GUI client from the NSM server.



NOTE: From release 2008.2 onwards, the GUI client connects with the GUI server on TCP port 7808. Earlier releases use TCP port 7801.

The following table describes the outbound ports on the NSM Management System.

Table 25: Outbound ports on the NSM Management System

Port	Protocol	Description
21	FTP	The port used to upload output to Juniper FTP when requesting technical support.
22	TCP	In an IP reachable workflow, the Device server uses this port to send commands to the device using SSH (a one-time connection).
23	TCP	In an IP reachable workflow, the Device server uses this port to send commands to the device using Telnet (a one-time connection).
25	TCP	If configured to send e-mail alerts, the Device server (SNMP client) connects to the SMTP server on this port.
53	UDP	During an attack database download, the Domain Name System (DNS) client resolves addresses using this port.
123	UDP	If Network Time Protocol (NTP) is used for clock synchronization, the Device server connects to the NTP server on this port.
161	UDP	The NSM Topology Discovery Manager uses SNMP to communicate with devices through this port.
162	UDP	The Device server sends SNMP traps to servers that listen on this port.
443	TCP	The Device server downloads the attack database and the Device Management Interface (DMI) schema using this port.
514	UDP	If configured, the Device server forwards logs in Syslog format to this port.
1645	UDP	If configured, the Device server connects to the RADIUS authentication server on this port.
1646	UDP	If configured, the Device server connects to the RADIUS accounting server using this port.
7801	TCP	The Device server communicates with the GUI server on this port
9020	UDP	If configured through NSM, a firewall uses this port for integrated surf control for Web filtering.

Using the Secure Server Protocol

NSM uses the Secure Server Protocol (SSP) to provide secure communication between management system components (GUI server and Device server), as well as between the Device server and the devices managed in your network. SSP offers strong encryption

and authentication mechanisms, so management traffic is protected and kept confidential. SSP utilizes RSA public key cryptography, AES symmetric encryption, and HMAC-SHA-1 hashing.

Communications with Devices Running ScreenOS 5.X and Later

If you are deploying NSM in a network with security devices running ScreenOS 5.0 and later, note that SSP uses two TCP ports for communication:

- Port 7800 between the Device server and the devices
- Port 7801 between the GUI server and the Device server.

You must allow TCP port 7800 on firewalls deployed between the NSM management system and the devices managed in your network. You must also configure firewalls between the GUI server and UI clients to permit TCP port 7808.

[Table 26 on page 280](#) lists and describes the ports used specifically in communications between NSM and ScreenOS 5.0 devices.

Table 26: Management System Communications With Devices Running ScreenOS

Server Component	Port	Description
Device server	Inbound TCP: 7800	Accepts incoming connections from devices running ScreenOS 5.0 and later.
Device server	Outbound TCP: 7801	Communicates with the GUI server.
Device server	Outbound TCP: 22/23	SSH/Telnet to import initial configurations of devices running ScreenOS 5.0 and later.
GUI server	Inbound TCP: 7808	Accepts communication from the GUI client.



NOTE: The Device server can use port 22 (SSH) to perform an initial connection to security devices running ScreenOS 5.0 and later, enabling you to set the NSM agent. The agent enables the device to communicate back to the Device server using SSP port 7800. Security devices running ScreenOS 5.0 and later, also support SSH v2.

Communications with Device Management Interface-Compatible Devices

If you are deploying NSM in a network with Device Management Interface (DMI)-compatible devices, such as Infranet Controller devices, Secure Access devices, J Series routers, and EX Series devices, two TCP ports are used for communication:

- Port 7804 between the Device server and the devices
- Port 7801 between the GUI server and the Device server.

You must allow TCP port 7804 on firewalls deployed between the NSM management system and the managed devices managed in your network. You must also configure firewalls between the GUI server and UI clients to permit TCP port 7808.

Table 27 on page 281 lists and describes the ports used specifically in communications between NSM and DMI-compatible devices.

Table 27: Management System Communications With DMI-Compatible Devices

Server Component	Port	Description
Device server	Inbound TCP: 7804	Accepts incoming device connections.
Device server	Outbound TCP: 7801	Communicates with the GUI server.
Device server	Outbound TCP: 22/23	SSH/Telnet to import initial configurations of DMI-compatible devices.
GUI server	Inbound TCP: 7808	Accepts communication from the GUI client.



NOTE: The Device server can use port 22 (SSH) to perform an initial connection to DMI-compatible devices, enabling you to set the NSM agent. The agent enables the device to communicate back to the Device server using port 7804.

Creating a Separate Management Network

We recommend that you isolate the NSM management system from the rest of your network traffic. You should send management traffic on a separate management network, and deploy a firewall to enforce access policies on the management network.

If you are deploying NSM in a network with DMI-compatible devices and security devices running ScreenOS 5.0 and later, then you must configure the firewall protecting the management network to allow:

- TCP ports 7800, 7803, and 7804 to the Device Servers.
- TCP port 22 outbound from the Device server.

You do not need to allow traffic to or from the GUI server if you deploy your UI clients inside the management network. If you must deploy UI clients outside the management network, then you must allow TCP port 7808 access to the GUI server in the firewall protecting the management network.

For management of devices, we recommend that you use SSP on the untrust interface, as this configuration reduces the possibility of losing access to the device due to an invalid configuration update.

APPENDIX B

Hardware Recommendations

This appendix lists guidelines for Network and Security Manager (NSM) hardware capacity. System requirements for each NSM component vary by use. We recommend that you discuss your current and projected device management requirements with a Juniper Networks Systems Engineer to ensure that your needs are met by the hardware you select.

These basic elements determine how much hardware you need:

- Type of installation: standalone or distributed
- Network Card Requirements
- Memory
- Storage capacity
- Processor speed

Specific requirements for each system vary, but you can apply some general rules and formulas.

This appendix contains these sections:

- [Standalone or Distributed System for GUI Server and Device Server on page 283](#)
- [Network Card Requirements on page 284](#)
- [Memory Requirements on page 284](#)
- [Storage Space Requirements on page 286](#)
- [Processor Speed Requirements on page 289](#)
- [Recommendations for Large-Scale Installations on page 290](#)

Standalone or Distributed System for GUI Server and Device Server

The GUI server and Device server may be combined in the same physical server if you have fewer than 200 devices, small device configuration sizes (for example, large number of NS-5GTs with a few larger systems), and fewer than 1000 logs per second from all devices.

For larger networks, we recommend distributing the GUI server and Device server.

Network Card Requirements

If you are managing more than 1000 devices, we recommend that you use two Network Interface Cards (NIC) for both GUI server and Device server systems. On each server, one of the NIC cards is dedicated for the connection with the other server. The other NIC card on the GUI server is used for UI connections. The other NIC card on the Device server is used for device connections.

Configuring Multiple Network Interface Cards

The process of configuring multiple Network Interface Cards (NICs) with NSM is as follows:

1. Before installing NSM, enable one NIC only.
2. Install NSM management system and User Interface.
3. Enable the second NIC.
4. Log into the UI as a superuser.
5. Select **Server Manager>Servers**.
6. Edit the Device server. Under the section MIP, add the IP Address of the second interface.
7. When you add a device, use the MIP Address for the devices to connect to the Device server.

Memory Requirements

This section details memory requirements on the GUI server and Device server.

GUI Server

A higher device configuration size requires more memory for the GUI server.

First, make note of the number and type of devices that will be managed by NSM, and their configuration sizes. Configuration sizes can vary widely based on the number of rules in a policy and the number of VPN tunnels. To determine configuration size for a device look at the first line of the output of `get config` on the CLI, or the equivalent Web UI action. This is the size of the configuration for a device in bytes. Take the sum of the configuration sizes to be managed, and see [Table 28 on page 284](#) to determine the estimated RAM required:

Table 28: GUI Server RAM Requirements

Total Config Size	GUI Server RAM Required
Less than 2 MB	4 GB
Between 2 and 10 MB	4 GB

Table 28: GUI Server RAM Requirements (continued)

Total Config Size	GUI Server RAM Required
Between 10 and 50 MB	6 GB
More than 50 MB	8 GB

After the installation, Juniper recommends that you make the following change on the server machine/(s):

In the `/var/netscreen/GuiSvr/guiSvr.cfg` file, change the value of `guiSvrDirectiveHandler.max.heap` from `1024000000` to `1536000000`. After implementing the change, restart Gui Svr.

Device Server

The key factor in determining the memory requirements for the Device server is the number of devices you are managing. Use [Table 29 on page 285](#) to determine the requirements for a given deployment size if the Device server is managing firewall/VPN devices or Junos devices.

Table 29: Device Server RAM Requirements for Firewall/VPN or Junos Devices

Number of Devices	Device Server RAM Required
Less than 200	4 GB
More than 200	6 GB

Use [Table 30 on page 285](#) to determine the requirements for a given deployment size if the Device server is managing IDP standalone devices that are performing profiling operations, Secure Access devices, or Infranet Controller devices.

Table 30: Device Server RAM Requirements for IDP, Secure Access, or Infranet Controller Devices

Number of Devices	Device Server RAM Required
1 through 3	4 GB
4 through 8	6 GB
9 through 30	8 GB

After the installation, Juniper recommends that you make the following change on the server machine/(s):

In the `/var/netscreen/DevSvr/devSvr.cfg` file, change the value of `devSvrDirectiveHandler.max.heap` from `1024000000` to `1536000000`. After implementing the change, restart Dev Svr.

UI Client

For managing a network with at least one DMI-compatible device in it, Juniper recommends a minimum of 2 GB of RAM. In addition, we recommend that you make the following change in the **NSM.lax** file in the **C:\Program Files\Network and Security Manager** directory on the client machines.

- For NSM 2009.1r1 release:

Change:

```
lax.nl.java.option.java.heap.size.max=384m
```

to:

```
lax.nl.java.option.java.heap.size.max=1280m
```

- For NSM 2010.1, 2010.2, and 2010.3 releases:

Change:

```
lax.nl.java.option.java.heap.size.max=768m
```

to:

```
lax.nl.java.option.java.heap.size.max=1280m
```

- For NSM 2010.4 and 2011.1 releases, the default maximum heap value is 1280m.

Storage Space Requirements

This section details storage space requirements on the GUI server and Device server.

GUI Server

The GUI server binaries and libraries require less than 100 MB.

Other key components that are disk space intensive are:

- Audit Log
- Error Log
- Device configuration database
- Nightly backup

The storage space requirements for each component are described in more detail below.

Audit Log

Configuring a greater level of detail in the audit log requires more disk space.

You can configure the level of detail in the **guiSvr.cfg** file located in **/usr/netscreen/GuiSvr** directory:

- To disable audit logging, set `guiSvrManager.auditlog_flag=0`.
- To enable summary audit logging, set `guiSvrManager.auditlog_flag=1` and `guiSvrManager.auditlog_detail_flag=0`.
- To enable detailed audit logging, set `guiSvrManager.auditlog_flag=1` and `guiSvrManager.auditlog_detail_flag=1`.

With audit logging enabled, more auditable events require more disk space as shown in [Table 31 on page 287](#).

Table 31: Audit Log Details

Operation	Audit Log Detail OFF	Audit Log Detail ON
Update Device 10K	408 bytes	40 KB
Update Device 30K	408 bytes	60 KB
Update Device 300K	456 bytes	240 KB
Add Device	6K	5 KB
Login in/out	540 bytes	180 bytes
Save Policy 25 rules	144 bytes	.01 MB
Save Policy 100 rules	192 bytes	0.5 MB
Save Policy 250 rules	1536 bytes	0.75 MB
Save Policy 1000 rules	3072 bytes	5 MB
Save Policy 5000 rules	6144 bytes	15 MB

For example, consider a system with 100 devices, with 10 KB configuration size per device, and 1000 rules, and this system has 100 device updates and 5 policies saves.

- With detailed audit logging enabled, the audit log will use:
 $100 * 40 \text{ KB} + 5 * 5 \text{ MB} = 29 \text{ MB}$ of disk space
- With the audit log details turned off, the audit log uses only:
 $100 * 408 \text{ bytes} + 5 * 1 \text{ KB} = 45 \text{ KB}$ of disk space.

The GUI server also requires 4 GB for the database transaction log.

Error Log

The `/var/netscreen/GuiSvr/errorLog` directory keeps error log files (`guidaemon.0`). It stores up to 25 files before the oldest log files are overwritten. Each day's file may be up to 5 MB in size. Based on these default settings, error logs can consume up to 125 MB (or 250 MB if the GUI server and the Device server are on the same server).

Device Configuration Database

The size of the Device Configuration database depends on the number of devices and types of configuration used. For every 1 MB of aggregate device configuration, NSM needs up to 200 MB of disk space.

For example, 100 devices with 10 KB configuration may need:

$(10 \text{ KB} * 100) * 200 = 200 \text{ MB}$ of disk space.

Nightly Backup

Nightly backup will maintain 7 copies of the GUI server database if the default installation option is selected. The disk space requirement should be $7 * (\text{device configuration database size calculated above})$.

Device Server Requirements

Storage capacity requirements are determined by the following equation:

$(\text{Retention period in days} * \text{Events per day} * 200 \text{ bytes}) / 1,000,000,000 = \text{storage size in GB.}$

Log events average around 200 bytes each. [Table 32 on page 288](#) lists some examples for a Device server managing just firewall/VPN devices based on a retention period of 30 days:

Table 32: Storage Requirements for Device Server Managing Firewall/VPN Devices

Events Per Day	Storage required
1,000,000	6 GB
10,000,000	60 GB
25,000,000	150 GB
50,000,000	300 GB

[Table 33 on page 289](#) lists some examples for a Device server managing just IDP stand-alone devices running profiler based on a retention period of 30 days:

Table 33: Storage Requirements for Device Server Managing IDP (w/Profiler) Devices

Number of Profiling Devices	Storage required
1 or 2	8 GB
3 through 8	12 GB
9 through 20	24 GB

Traffic logs make up about 2/3 of all logs. Turning off traffic logs can result in a large savings in storage space.

In NSM, logs are stored in `/var/netscreen` directory of the Device server by default. Always mount the `/var` directory on a separate partition or drive from `/` to avoid log files filling up your root partition and crashing your server. In situations calling for high volume logging, we recommend you mount `/var` on a locally attached high speed SCSI drive or similar performance storage solution. You can specify the path for log storage during initial installation.

In addition to regular logs, error logs may consume up to 125 MB of storage space on the Device server.

Processor Speed Requirements

This section details requirements for CPU on the GUI server and Device server.

GUI Server

A faster CPU in the GUI server provides for a more responsive Log Viewer, and a more responsive system overall. We recommend that you focus on a system that supports your storage and memory needs first, and get a mid-range to high-end processor for it. Dual processors in the GUI server have a negligible performance benefit for NSM, but might have additional performance benefits with future releases.

Device Server Managing IDP Standalone Devices Running Profiler

More CPUs enable the Device server to manage more IDP standalone devices running profiler. See [Table 34 on page 289](#).

Table 34: CPU Requirements for Device Server Managing IDP (w/Profiler) Devices

Number of Profiling Devices	CPUs
1 or 2	1
3 through 8	2
9 through 20	4

Recommendations for Large-Scale Installations

The following recommendations apply for large-scale installations of NSM:

- Install Linux ext2 filesystem for maximum performance. Note that without journaling, crash recovery will not be robust. Regular backups mitigate that risk.
- Disable atime filesystem feature by mounting the noatime option.
- Use secondary 7200 RPM or better SATA hard drive for **/var/netscreen** on both GUI server and Device server.
- For maximum server capacity and performance, use a high performance RAID controller such as the Adaptec 2410SA with striping across 2 or more 10,000 RPM drives. Avoid LSI MegaRAID based adapters (commonly shipped with Dell servers) since these have performed poorly in our internal testing.
- The Device server must have at least enough space in **/var/netscreen** for 1 day of logs. Make sure that the storage manager parameters in **devSvr.cfg** are adjusted to cover one full day's worth of logs. You should set values in both the `storageManager.minimumFreeSpace` and `storageManager.alert` parameters to the same value (in MB). Recommended is 2 or more days' space for logs.

APPENDIX C

Profiler Performance Tuning Recommendations

This appendix provides performance tuning guidelines for running the Profiler when managing IDP standalone sensors in Network and Security Manager (NSM).

- [Performance Tuning Recommendations on page 291](#)
- [Setting Preferences to Improve Profiler Performance on page 294](#)

Performance Tuning Recommendations

The following performance tuning recommendations are based on the number of IDP standalone sensors that you have configured to perform Profiling activities:

- Low-End Configuration (1 or 2 profiling devices)
- Medium-Sized Configuration (3 through 8 profiling devices)
- High-End Configuration (9 through 20 profiling devices)

Recommendations for Low-End Configurations:

[Table 35 on page 291](#) describes recommendations for optimum performance when managing one to two profiling devices.

Table 35: Performance Tuning Recommendations for Low-End Configurations

Component	Recommended	Value
Server Setup	GUI server and Device server (NSM Profiler DB) running on the same machine	N/A
	Physical Memory Required	1 GB
	CPU	1 Fast
	Disk space reserved for Profiler	8 GB
UI System Preferences	Purge profiler database if size exceeds	1000 MB

Table 35: Performance Turning Recommendations for Low-End Configurations (continued)

Component	Recommended	Value
	Max profiler database size after purging	750 MB
PostgreSQL Settings	shared_buffers	1000 KB for Linux
		700 KB for Solaris
	work_mem	16384 KB
	maintenance_work_mem	8192 KB
	max_fsm_pages	20000 disk pages
	checkpoint_segments	64 log file segments
	checkpoint_timeout	600 seconds
Device server	profilerMgr.receiver.maxParallelConns	Reduce from 3 to 1

See “[Setting Preferences to Improve Profiler Performance](#)” on page 294 for more information on recommended settings.

Medium-Size Configuration (3 to 8 IDP Profiling Devices)

[Table 36 on page 292](#) describes recommendations for optimum performance when managing 3 to 8 profiling devices.

Table 36: Performance Turning Recommendations for Medium-Sized Configurations

Component	Recommended	Value
Server Setup	GUI server and Device server (NSM Profiler DB) running on the same machine	N/A
	Physical Memory Required	4 GB
	CPU	2 Fast
	Disk space reserved for Profiler. *High-end SCSI drives preferred	12 GB
UI System Preferences	Purge profiler database if size exceeds	3000 MB
	Max profiler database size after purging	2200 MB
PostgreSQL Settings	shared_buffers	32768 KB
	work_mem	32768 KB

Table 36: Performance Turning Recommendations for Medium-Sized Configurations (continued)

Component	Recommended	Value
	maintenance_work_mem	32768 KB
	max_fsm_pages	200000 disk pages
	checkpoint_segments	64 log file segments
	checkpoint_timeout	600 seconds
Device server	profilerMgr.receiver.maxParallelConns	Reduce from 3 to 1

See [“Setting Preferences to Improve Profiler Performance” on page 294](#) for more information on recommended settings.

High-End Configuration (9 to 20 IDP Profiling Devices)

[Table 37 on page 293](#) describes recommendations for optimum performance when managing 9 to 20 profiling devices.

Table 37: Performance Turning Recommendations for High-End Configurations

Component	Recommended	Value
Server Setup	GUI server and Device server (NSM Profiler DB) running on the separate machines	N/A
	Physical Memory Required	8 GB
	CPU	4 Fast
	Disk space reserved for Profiler. *High-end SCSI drives preferred	24 GB
UI System Preferences	Purge profiler database if size exceeds	8000 MB
	Max profiler database size after purging	6000 MB
PostgreSQL Settings	shared_buffers	262143 KB
	work_mem	512000 KB
	maintenance_work_mem	32768 KB
	max_fsm_pages	2000000 disk pages
	checkpoint_segments	128 log file segments

Table 37: Performance Turning Recommendations for High-End Configurations (continued)

Component	Recommended	Value
	checkpoint_timeout	3600 seconds

See “[Setting Preferences to Improve Profiler Performance](#)” on page 294 for more information on recommended settings.

Setting Preferences to Improve Profiler Performance

Additional information on recommended settings is provided for the following system components to improve the performance of the Profiler when managing IDP standalone sensors in NSM:

- User Interface (UI) System Preferences
- PostgreSQL Server
- Operating System Shared Memory Requirements
- Device server

UI System Preferences

From the UI, use System Preferences > Profiler Settings to configure settings on the Profiler to improve performance. [Table 38 on page 294](#) describes settings that you can configure to improve performance from the UI.

Table 38: Profiler Settings in UI System Preferences

Parameter	Description	Default Value
DB Max Size—Purge Profiler Database if size exceeds (in MB)	A background Auto Purge is triggered if the Profiler database size exceeds this limit.	3000 MB
DB Max Size After Purge	Auto Purge attempts to bring down the Profiler database size to less than this limit.	2200 MB
Profiler Query Timeout (in seconds)	The SQL query timesout when this interval is elapsed, irrespective of whether the entire database is searched or not. In the event of a timeout, the result available so far is returned.	120 seconds
Hour of day to perform database optimization (local time)	Database optimization is complex operation. It occurs at or around the specified hour of day. We recommend that you set this setting to an hour of the day when user activities are at a minimum, such as midnight local time. The time is displayed as local time of the NSM UI client. If you have multiple clients operating at varying time zones, you must set this value to minimize the effect of the optimization operation.	7 GMT

PostgreSQL Server

You can also configure settings on the PostgreSQL server to improve the performance of the NSM Profiler DB. These settings appear in the following file on the Device server:

```
$NSROOT/DevSvr/var/pgsql/data/postgresql.conf
```

Most of the changes to improve PostgreSQL performance will increase the shared memory requirement described in the next section.

[Table 39 on page 295](#) describes parameters in the **postgresql.conf** file that affect Profiler performance.

Table 39: PostgreSQL Server Settings

Parameter	Description	Default Value
shared_buffers	Sets the number of shared memory buffers (each 8 KB) used by the database server. Minimum is 2 X max_connections	1000 KB
work_mem	Specifies the amount of memory to be used by internal sorts and hashes before switching to temporary disk files. The value is specified in kilobytes.	16384 KB
maintenance_work_mem	Specifies the maximum amount of memory to be used in maintenance operations, such as VACUUM. The value is specified in kilobytes.	8192 KB
max_fsm_pages	Sets the maximum number of disk pages for which free space is tracked in the shared free-space map. Six bytes of shared memory are consumed for each page slot.	20000
checkpoint_segments	Maximum distance between automatic checkpoints maintained by postgresql, in log file segments.	64
checkpoint_timeout	Maximum time between automatic checkpoints, in seconds.	600 seconds

The defaults mentioned here are configured by NSM during initial installation. In some cases, the actual PostgreSQL default values are not indicated.

Shared Memory

When you configure the PostgreSQL server to perform better with more shared memory, the devSvrDbSvr (postmaster) process may not come up if the system does not support

it. In such cases, after a failed run of `devSvrDbSvr`, you can identify the actual memory requirement from the following file:

```
$NSRROOT/DevSvr/var/pgsql/data/psql.log file
```

The error appears as follows:

```
"Failed system call was shmget(key=5432001, size=145408000, 03600)"
```

Note that size specifies the required shared memory. You can then update the shared memory requirement.

On Solaris systems, add/update the following line in `/etc/system`:

```
set shmsys:shminfo_shmmax=<required shared mem>'
set shmsys:shminfo_shmmni=1
set shmsys:shminfo_shmseg=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semsl=32
```

On Linux systems, add/update the following line in `/etc/sysctl.conf`:

```
kernel.shmmax=<required shared mem>'
```

After updating the shared memory requirements, you must restart the system.

Device Server

You can also configure settings on the Device server to improve the performance of the NSM Profiler DB. [Table 40 on page 296](#) describes parameters in the Device server configuration file (`devSvr.cfg`) that affect performance.

Table 40: Device Server Settings

Parameter	Description	Default Value
profilerMgr.printLevel	For debugging, info is most useful, but will potentially generate lots of logs.	Notice
profilerMgr.receiver.pktIntTimeoutInSec	A profiler session times out of time exceeds this configured value.	300 seconds

Table 40: Device Server Settings (continued)

Parameter	Description	Default Value
profilerMgr.receiver.saveFailedData	Profiler Data of a profiler session is stored temporarily in the folder . <code>\$NSROOT/DevSvr/var/profiler_data/domainId.deviceId.sessionId</code> If a session completes successfully this folder is cleaned up. Otherwise, the folder is cleaned up unless this setting is 'YES'.	NO
profilerMgr.receiver.maxParallelConns	Specifies maximum number of concurrent profiler sessions.	3
profilerMgr.receiver.minPollTimeInSec	Two consecutive profiler sessions for the same device is spaced apart by at least this interval.	300 seconds
profilerMgr.receiver.vacuumCostDelay	The length of time, in milliseconds, that the vacuum process will sleep when the vacuumCostLimit has been exceeded.	0 msec
profilerMgr.receiver.vacuumCostLimit	The accumulated cost that will cause the vacuuming process to sleep.	200 msec
profilerMgr.receiver.minVacuumInterval	Minimum time interval between two consecutive vacuums.	300 seconds
profilerMgr.receiver.performVacuumFull	If this setting is 'YES', VACUUM FULL is performed during optimization otherwise skipped.	NO
profilerMgr.receiver.optimizationWindow	This specifies the time window in hours from the 'hour to perform optimization' setting of GUI >System Preferences >Profiler Settings. Optimization would be triggered only during this window.	3 hours
profilerMgr.profilerQuerier .profilerQueryTimeoutInterval	A GUI query session is timed out if there is no activity for this interval.	600 seconds

NSM Generated Logs' Impact on Performance

If you notice “Could not write the whole buffer to FIFO” entries in the deviceDaemon log files, we recommend that you turn off NSM generated logs by unchecking the “New Host” , “New Protocol” , and “New Port” detected check boxes in the IDP device editor, and save the data. Excessive messages indicating “Could not write the whole buffer to FIFO” could indicate that Device server performance is affected by these NSM generated logs.

GUI Server

You can also configure settings on the GUI server to improve database access performance. To do so, modify the `set_cachesize` parameter in the `/var/netscreen/GuiSvr/var/xdb/data/DB_CONFIG` according to available system memory and CPU numbers. For example, on scale test bed (with 8 GB RAM and 4 CPUs), we recommend that you set this value as follows:

```
set_cachesize 0 1024000000 4
```

If you need more memory, change the BDB config to increase the exiting limit. Increase the parameters listed below in the `/var/netscreen/GuiSvr/xdb/data/DB_CONFIG` file.

```
set_data_dir .
set_lg_dir ../log
set_lg_regionmax 600000
set_lk_max_lockers 200000
set_lk_max_locks 200000
set_lk_max_objects 200000
set_cachesize 0 1024000000 1
```