END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT (“AGREEMENT”) BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software (“Customer”) (collectively, the “Parties”).

2. The Software. In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

   a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

   b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

   c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer’s use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities; or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer’s use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

   d. For any trial copy of the Software, Customer’s right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

   e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer’s enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any ‘locked’ or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the
Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer’s internal business purposes.

7. **Ownership.** Juniper and Juniper’s licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the “Warranty Statement”). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper’s or its suppliers’ or licensors’ liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer’s possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly providing Juniper with valid tax receipts and other required documentation showing Customer’s payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer’s non-compliance or delay with its responsibilities herein. Customer’s obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer’s ability to export the Software without an export license.
12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer’s written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at [http://www.gnu.org/licenses/gpl.html](http://www.gnu.org/licenses/gpl.html), and a copy of the LGPL at [http://www.gnu.org/licenses/lgpl.html](http://www.gnu.org/licenses/lgpl.html).

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s’y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).
# Table of Contents

**About This Guide** ................................................. xvii

- Objectives .......................................................... xvii
- Audience ............................................................. xvii
- Conventions .......................................................... xvii
- Documentation ....................................................... xix
- Requesting Technical Support ........................................ xx
  - Self-Help Online Tools and Resources ......................... xxi
  - Opening a Case with JTAC ........................................ xxi

**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 ............................ 7
  - Standalone Configuration .......................................... 8
  - Distributed Configuration .......................................... 8
  - Simple High Availability Configuration ............................ 9
  - Extended High Availability Configuration .......................... 9
- Other Configuration Options ............................................ 9
  - Local/Remote Database Backup ..................................... 10
  - NetScreen-Statistical Report Server Interoperability .............. 10
  - Device Server Database ........................................... 11
- Next Steps ............................................................. 11

**Chapter 2** Generating the NSM License Key File ........................................ 13

- Installing NSM for the First Time ....................................... 13
  - NSM Trial Licenses .................................................... 14
  - Generating the License Key for an NSM Software-Only Installation ....................... 14
  - Generating the License Key for an NSM Appliance Installation ......................... 14
  - Generating the License Key for a High Availability NSM Installation .................. 14
- Upgrading to an NSM Release that Requires a License .......................... 15
  - Generating the License Key for an NSM Software-Only Upgrade ....................... 15
  - Generating the License Key for an NSM Appliance Upgrade Installation .............. 16
  - Generating the License Key File for an NSM 2007.3 or Later High Availability Upgrade Installation .......................... 16
Upgrading NSM in a Standalone Configuration .......................... 140
  Typical Output for a Standalone Upgrade .......................... 145
  Starting Server Processes Manually .............................. 148
  Validating Management System Status ............................ 149
Upgrading the User Interface ........................................ 149
  Downloading and Installing the UI Client Automatically .......... 149
  Downloading and Installing the UI Client Manually .............. 150
  Validating the Upgrade .......................................... 150
Upgrading NSM in a Distributed Configuration ..................... 150
Upgrading NSM with HA Enabled ....................................... 151
  Upgrading the Database Backup Files ............................. 153
Restoring Data if the Upgrade Fails ................................ 153
Next Steps ............................................................ 154

Chapter 7  Upgrading NSMXpress and NSM Central Manager to NSM 2009.1 ...... 155
  Upgrading NSMXpress and NSMCM Appliances ...................... 155
  Upgrading to NSM 2009.1 Release on an NSM Appliance .......... 155
  Upgrading to NSM 2009.1 Release on an NSM Central Manager Appliance ........................................ 157
  Upgrading to NSM 2009.1 Release on an NSMXpress Appliance (Offline Mode) ........................................ 160
  Upgrading to NSM 2009.1 Release on an NSM Central Manager Appliance (Offline Mode) ...................... 162
NSMXpress Data Migration ............................................... 165
  Solaris to NSMXpress Data Migration ............................. 165
    On the Solaris server: .......................................... 165
    On the NSMXpress appliance: .................................. 166
  Linux to NSMXpress Data Migration .............................. 167
    On the Linux Server ............................................ 168
    On an NSMXpress Appliance ................................... 168
User Privileges on NSMXpress .......................................... 169

Chapter 8  Maintaining NSM ................................................. 171
  Controlling the Management System ............................... 171
    Viewing Management System Commands ........................ 171
    Common Management System Commands ........................ 172
    Starting All Server Processes Using the HA Server .......... 172
    Starting GUI Server and Device Server Processes Manually ........................................................................ 173
    Stopping Server Processes ....................................... 173
Configuring Server Options .......................................... 173
  Changing the Management System IP Address .................... 174
  Changing the Device Server IP Address ........................... 174
  Changing the GUI Server IP Address ............................... 175
Configuring Disk Space Management on the Device Server ........ 175
Configuring Disk Space Management on the GUI Server ........ 176
Configuring Connection Timing ........................................ 177
Setting Core File Naming on Solaris ................................ 177
Archiving and Restoring Logs and Configuration Data ............ 178
  Archiving Logs and Configuration data .......................... 178
  Restoring Logs and Configuration Data ........................... 179
## List of Figures

<table>
<thead>
<tr>
<th>Part 1</th>
<th>Network and Security Manager Installation Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 3</td>
<td>Installing NSM in a Standalone Configuration ................. 21</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Installing NSM with High Availability ...................... 71</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Technical Overview of the NSM Architecture ............... 193</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UI Installer Introduction Screen 41</td>
</tr>
<tr>
<td>2</td>
<td>UI Installation—Choose Install Folder 42</td>
</tr>
<tr>
<td>3</td>
<td>UI Installation—Choose Shortcut Folder 43</td>
</tr>
<tr>
<td>4</td>
<td>UI Installation—Preinstallation Summary 44</td>
</tr>
<tr>
<td>5</td>
<td>Validating the NSM Installation 46</td>
</tr>
<tr>
<td>6</td>
<td>Simple HA Management System Configuration 72</td>
</tr>
<tr>
<td>7</td>
<td>HA Configuration Example 96</td>
</tr>
<tr>
<td>8</td>
<td>Configuring the HA GUI Server Cluster 108</td>
</tr>
<tr>
<td>9</td>
<td>Configuring the HA Device Server Cluster 109</td>
</tr>
<tr>
<td>10</td>
<td>Configuring e-mail Notification 110</td>
</tr>
<tr>
<td>11</td>
<td>Extended HA Configuration Example 112</td>
</tr>
<tr>
<td>12</td>
<td>NSM Architecture 193</td>
</tr>
<tr>
<td>13</td>
<td>NSM Management System 194</td>
</tr>
</tbody>
</table>
List of Tables

About This Guide ................................................. xvii
Table 1: Notice Icons .............................................. xviii
Table 2: Text Conventions ........................................... xviii
Table 3: Syntax Conventions ....................................... xix
Table 4: Network and Security Manager Publications ............... xix

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  Generating the NSM License Key File .................... 13
Table 9: Licensing FAQ ............................................ 19

Chapter 3  Installing NSM in a Standalone Configuration .......... 21
Table 10: Common System Parameters .......................... 22

Chapter 4  Installing NSM in a Distributed Configuration .......... 49
Table 11: Distributed Configuration — System Parameters ........ 50

Chapter 5  Installing NSM with High Availability ................... 71
Table 12: HA Utilities ............................................. 77
Table 13: Simple HA Configuration — System Parameters .......... 80
Table 14: Extended HA Configuration — System Parameters ....... 83
Table 15: Shared Disk System Parameters ........................ 83
Table 16: Useful Installation and Troubleshooting Commands ........ 94

Chapter 6  Upgrading to NSM 2009.1 from an Earlier Version ....... 131
Table 17: Standalone Configuration—System Parameters .......... 132
Table 18: Distributed Configuration — System Parameters .......... 134
Table 19: HA Configuration — System Parameters ................ 134
Table 20: Shared Disk Parameters .................................. 136

Chapter 8  Maintaining NSM ....................................... 171
Table 21: Management System Commands ........................ 172

Part 2  Appendixes

Appendix A  Technical Overview of the NSM Architecture ........ 193
About This Guide

- Objectives on page xvii
- Audience on page xvii
- Conventions on page xvii
- Documentation on page xix
- Requesting Technical Support on page xx

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 xviii defines notice icons used in this guide.
**Table 1: Notice Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Informational note icon" /></td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td><img src="image" alt="Caution icon" /></td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td><img src="image" alt="Warning icon" /></td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td><img src="image" alt="Laser warning icon" /></td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>

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

**Table 2: Text Conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold typeface like this</strong></td>
<td>Represents commands and keywords in text.</td>
<td>Issue the <code>clock source</code> command.</td>
</tr>
<tr>
<td></td>
<td>Represents keywords</td>
<td>Specify the keyword <code>exp-msg</code>.</td>
</tr>
<tr>
<td></td>
<td>Represents UI elements</td>
<td>Click User Objects</td>
</tr>
<tr>
<td><strong>Bold typeface like this</strong></td>
<td>Represents text that the user must type.</td>
<td>user input</td>
</tr>
<tr>
<td><strong>fixed-width font</strong></td>
<td>Represents information as displayed on the terminal screen.</td>
<td><code>host1# show ip ospf</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Routing Process OSPF 2 with Router ID 5.5.0.250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router is an area Border Router (ABR)</td>
</tr>
<tr>
<td><strong>Key names linked with a plus (+) sign</strong></td>
<td>Indicates that you must press two or more keys simultaneously.</td>
<td>Ctrl + d</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Emphasizes words</td>
<td>The product supports two levels of access, user and privileged.</td>
</tr>
<tr>
<td></td>
<td>Identifies variables</td>
<td><code>clusterID, ipAddress</code>.</td>
</tr>
<tr>
<td><strong>The angle bracket (&gt;)</strong></td>
<td>Indicates navigation paths through the UI by clicking menu options and links.</td>
<td>Object Manager &gt; User Objects &gt; Local Objects</td>
</tr>
</tbody>
</table>

Table 3 on page xix defines syntax conventions used in this guide.
Table 3: Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in plain text</td>
<td>Represent keywords</td>
<td>terminal length</td>
</tr>
<tr>
<td>Words in italics</td>
<td>Represent variables</td>
<td>mask, accessListName</td>
</tr>
<tr>
<td>Words separated by the pipe (</td>
<td>) symbol</td>
<td>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.</td>
</tr>
<tr>
<td>Words enclosed in brackets ( [ ] )</td>
<td>Represent optional keywords or variables.</td>
<td>[ internal</td>
</tr>
<tr>
<td>Words enclosed in brackets followed by an asterisk ([ ]*)</td>
<td>Represent optional keywords or variables that can be entered more than once.</td>
<td>[ level1</td>
</tr>
<tr>
<td>Words enclosed in braces ( { } )</td>
<td>Represent required keywords or variables.</td>
<td>{ permit</td>
</tr>
</tbody>
</table>

Documentation

Table 4 on page xix describes documentation for NSM.

Table 4: Network and Security Manager Publications

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network and Security Manager Installation Guide</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Network and Security Manager Administration Guide</strong></td>
<td>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. 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.</td>
</tr>
<tr>
<td><strong>Network and Security Manager Configuring ScreenOS Devices Guide</strong></td>
<td>Provides details about configuring device features for all supported ScreenOS platforms.</td>
</tr>
<tr>
<td><strong>Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide</strong></td>
<td>Provides details about configuring device features for all supported Intrusion Detection and Prevention (IDP) platforms.</td>
</tr>
</tbody>
</table>
Table 4: Network and Security Manager Publications (continued)

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network and Security Manager Online Help</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Network and Security Manager API Guide</strong></td>
<td>Provides complete syntax and description of the SOAP messaging interface to NSM.</td>
</tr>
<tr>
<td><strong>Network and Security Manager Release Notes</strong></td>
<td>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. Release notes are included on the corresponding software CD and are available on the Juniper Networks website.</td>
</tr>
<tr>
<td><strong>Network and Security Manager Configuring Infranet Controllers Guide</strong></td>
<td>Provides details about configuring the device features for all supported Infranet Controllers.</td>
</tr>
<tr>
<td><strong>Network and Security Manager Configuring Secure Access Devices Guide</strong></td>
<td>Provides details about configuring the device features for all supported Secure Access Devices.</td>
</tr>
<tr>
<td><strong>Network and Security Manager Configuring EX Series Switches Guide</strong></td>
<td>Provides details about configuring the device features for all supported EX Series platforms.</td>
</tr>
<tr>
<td><strong>Network and Security Manager Configuring J Series Services Routers and SRX Series Services Gateways Guide</strong></td>
<td>Provides details about configuring the device features for all supported J Series Services Routers and SRX Series Services Gateways.</td>
</tr>
<tr>
<td><strong>Network and Security Manager M Series and MX Series Devices Guide</strong></td>
<td>Provides details about configuring the device features for M Series and MX Series platforms.</td>
</tr>
</tbody>
</table>

**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 JNASC 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.

- Product warranties—For product warranty information, visit [http://www.juniper.net/support/warranty/](http://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: http://www.juniper.net/customers/support/
• Find product documentation: http://www.juniper.net/techpubs/
• Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
• Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
• Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
• Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
• Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

• Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
• 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, visit us at http://www.juniper.net/support/requesting-support.html
Network and Security Manager Installation Procedures

- Introduction on page 3
- Generating the NSM License Key File on page 13
- Installing NSM in a Standalone Configuration on page 21
- Installing NSM in a Distributed Configuration on page 49
- Installing NSM with High Availability on page 71
- Upgrading to NSM 2009.1 from an Earlier Version on page 131
- Upgrading NSMXpress and NSM Central Manager to NSM 2009.1 on page 155
- Maintaining NSM on page 171
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 7
• Other Configuration Options on page 9
• Next Steps on page 11

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 201.

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 script 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 computer 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 located on the NSM installation CD or on the Internet at the Juniper Networks corporate support 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 CD.

Table 5: NSM Installation Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsm2009.1_ui_win_x86.exe</td>
<td>Installer for the NSM UI (for Windows-based computers).</td>
</tr>
<tr>
<td>nsm2009.1_ui_linux_x86.bin</td>
<td>Installer for the NSM UI (for Linux-based computers).</td>
</tr>
<tr>
<td>nsm2009.1_servers_linux_x86.sh</td>
<td>Installer for the NSM management system for Linux.</td>
</tr>
<tr>
<td>nsm2009.1_servers_sol_sparc.sh</td>
<td>Installer for the NSM management system for Solaris.</td>
</tr>
</tbody>
</table>
Table 5: NSM Installation Files (continued)

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsm2009r1-systemupdate-linuxES_4.tar</td>
<td>System update utility for RHEL ES 4.0. Use this file to update files on your system required for the installer to run properly.</td>
</tr>
<tr>
<td>nsm2009r1-systemupdate-linuxES_5.tar</td>
<td>System update utility for RHEL ES 5.0. Use this file to update files on your system required for the installer to run properly.</td>
</tr>
<tr>
<td>nsm2009r1-systemupdate-solaris10.tar</td>
<td>System update utility for Solaris 10. Use this file to update files on your system required for the installer to run properly.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Solaris 10 operating system, or RHEL 32-bit ES/AS 4.0-Update 7 or 32-bit ES/AS 5.0-Update 3 (Minimal and Full Install)</td>
</tr>
<tr>
<td>CPU</td>
<td>Only Sun Microsystems UltraSPARC III 1 GHz or UltraSPARC T2; or Linux 2 GHz (x86) processor (or higher)</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
</tr>
<tr>
<td>Swap Space</td>
<td>4 GB for both GUI Server and Device Server</td>
</tr>
<tr>
<td>Storage</td>
<td>Hard Disk Drive with 7,200 RPM (minimum); 15,000 RPM (recommended); 40 GB disk space (minimum); 80 GB disk space (recommended)</td>
</tr>
<tr>
<td></td>
<td>By directory:</td>
</tr>
<tr>
<td></td>
<td>• /usr—7 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• /var—10 GB min</td>
</tr>
<tr>
<td></td>
<td>• /tmp—2 GB minimum</td>
</tr>
<tr>
<td>Network Connection</td>
<td>100 Mbps (minimum) Ethernet adapter; higher speeds are recommended</td>
</tr>
</tbody>
</table>
Table 6: Minimum System Requirements—Management System on Same Server (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Solaris 10 operating system, or RHEL 32-bit ES/AS 4.0-Update 7 or 32-bit ES/AS 5.0-Update 3 (Minimal and Full Install)</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: 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.</td>
</tr>
<tr>
<td>CPU</td>
<td>Only Sun Microsystems UltraSPARC IIi 1GHz (or higher), OR Linux 2 GHz (x86) processor (or higher)</td>
</tr>
<tr>
<td>RAM</td>
<td>2GB</td>
</tr>
<tr>
<td>Swap Space</td>
<td>2GB for the GUI Server, 2 GB for the Device Server</td>
</tr>
<tr>
<td>Storage</td>
<td>Hard Disk Drive with 7,200 RPM (minimum); 15,000 RPM (recommended); 40 GB disk space (minimum); 80 GB disk space (recommended)</td>
</tr>
<tr>
<td></td>
<td>By directory:</td>
</tr>
<tr>
<td></td>
<td>• <code>/usr</code>—7 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• <code>/var</code>—10 GB min</td>
</tr>
<tr>
<td></td>
<td>• <code>/tmp</code>—2 GB minimum</td>
</tr>
<tr>
<td>Network Connection</td>
<td>100 Mbps (minimum) Ethernet adapter; higher speeds are recommended</td>
</tr>
<tr>
<td>Device Connection bandwidth to NSM</td>
<td>56 Kbps (minimum)</td>
</tr>
<tr>
<td>Other</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>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 only</td>
</tr>
<tr>
<td>Hardware</td>
<td>IBM compatible PC</td>
</tr>
<tr>
<td></td>
<td>Pentium 4 or equivalent</td>
</tr>
<tr>
<td></td>
<td>RAM: 1 GB.</td>
</tr>
<tr>
<td></td>
<td>384 Kbps (DSL) or LAN connection — minimum bandwidth required to connect to the NSM management system.</td>
</tr>
</tbody>
</table>

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 6000 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 201.

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 8
- Distributed Configuration on page 8
- Simple High Availability Configuration on page 9
- Extended High Availability Configuration on page 9

**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 installer script 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 installer script 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 71.

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 installer script prompts you to specify whether this server machine requires local database backups. If you choose to do so, the installer script 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 installer script 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 installer script 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 installer script 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 user name
Database password

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


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

Device Server Database

The 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 installer creates the user for you. In this case, the 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 21—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 71—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 2009.1 from an Earlier Version” on page 131—includes specific information describing how to upgrade previous installations of NSM to this version.

• “Maintaining NSM” on page 171—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.
In Release 2007.3 and later releases, the NSM product line uses a licensing mechanism to prevent access to an unlicensed copy of NSM and to enforce a limit on the maximum number of devices that can be managed by NSM. New installations and installations upgrading from a release prior to 2007.3 must obtain a license to use NSM.

The base license supports 25 devices with high availability (HA), including devices running ScreenOS, IDP, or JUNOS Software with Enhanced Services; EX Series, Secure Access, or Infranet Controller devices; and including any modeled or vsys devices. For details on these devices, see the Network and Security Manager Administration Guide.

To manage more than 25 devices, a license key must be purchased separately, retrieved from the Juniper License Management Server (LMS), and then installed onto the NSM Server or NSM appliance.

LMS provides an interface to generate licenses based upon serial number, authorization code and installation ID.

Procedures provided in the following sections use the Installer to generate the installation ID. Alternatively, you can download a utility from the Juniper Networks Software Download site for generating the installation ID.

- Installing NSM for the First Time on page 13
- Upgrading to an NSM Release that Requires a License on page 15
- Example of an NSM License File on page 17
- Installing the License Key File in Various Configurations on page 18
- Upgrading the License Key on page 18
- Viewing License Key Information on page 18
- Enforcing Licenses on page 18
- Licensing FAQ on page 19

**Installing NSM for the First Time**

The first time you install NSM 2007.3 or later release software only, you need to generate a license key file that requires an installation ID.
NSM Trial Licenses

You can generate a trial license for NSM for periods of 30, 60 or 90 days. The NSM License Information dialog box displays the validity period in the Expires in (Days) field. Licenses can only be installed or updated from the NSM GUI. When the trial period is over, NSM notifies you and prompts you to install a new license. If you install the new license, you can proceed to log in to NSM. If not, you must exit from the GUI.

Generating the License Key for an NSM Software-Only Installation

To generate the license key file for an NSM 2007.3 or later software-only installation:

1. Run the installer image on the server designated for NSM. The NSM Server generates an installation ID.
2. Log in to the LMS system and select License key generation for NSM.
3. Enter the serial number and authorization code.
   Your serial number is printed on the paper license certificate given to you when you purchased NSM.
   Depending on the package you purchased, Juniper Networks provides an authorization code by e-mail. If you received a paper license certificate, and are managing more than 25 devices, call Juniper Networks Customer Service. The Customer Service will validate your purchase and generate a license key file.
4. Enter the installation ID that was generated by the NSM Server.
   The LMS system generates a license key file for the SKU recorded. You can choose to download the licence key file, or to receive it by email.
5. Save the license key file to your local drive for use during installation.

Generating the License Key for an NSM Appliance Installation

To generate the license key file for an NSM appliance installation:

1. Log in to the LMS system and select License key generation for NSM.
2. Enter the serial number and authorization code.
   The serial number is on the back of the NSM appliance chassis.
   Depending on the package you purchased, Juniper Networks provides an authorization code via e-mail. If you received a paper license certificate, and are managing more than 25 devices, call Juniper Networks Customer Service. Customer Service will validate your purchase and generate a license key.
   The LMS system generates a license key file for the SKU recorded. You can choose to download the licence key file, or to receive it by email.
3. Save the license key file to your local drive for use during installation.

Generating the License Key for a High Availability NSM Installation

To generate the license key file for an NSM 2007.3 or later HA installation:
1. Run the NSM installer image on the server designated as your primary NSM (or primary GUI Server). The NSM Server generates an installation ID.

2. Run the NSM 2007.3 or later installer image on the server designated as your secondary NSM (or secondary GUI Server). The NSM Server generates an installation ID.

3. Log in to the LMS system and select License key generation for NSM.

4. Enter the serial number and authorization code of your primary NSM.

   For an NSM appliance installation, enter the serial number of the primary server. The hardware serial number is located on the back of the NSM appliance chassis.

   For a software-only installation:
   
   a. Enter the serial number.

   The serial number of your software is printed on the paper license certificate given to you when you purchased NSM. If you do not have the software serial number or the LMS System fails to recognize the serial number, call Juniper Networks Customer Service.

   b. Enter the installation ID of the primary NSM.

   Depending on the package you purchased, Juniper Networks provides an authorization code via e-mail. If you received a paper license certificate, and are managing more than 25 devices, call Juniper Networks Customer Service. Customer Service will validate your purchase and generate a license key.

5. Select the Need High Availability Key check box. The LMS systems prompts you to provide the NSM Secondary serial number and Secondary Installation ID.

   The LMS system generates a license key file for the SKU recorded. You can choose to download the file, or to receive it by email.

6. Save the license key file to your local drive for use during installation.

Upgrading to an NSM Release that Requires a License

When you upgrade to a NSM 2007.3 or later release from a version that is older than 2007.3, you need to generate a license key file that requires an installation ID.

Generating the License Key for an NSM Software-Only Upgrade

To generate the license key file to upgrade to NSM 2007.1 or later release:

1. Run the NSM installer image on the server designated for NSM. The NSM Server generates an installation ID.

2. Log in to the LMS system and select License key generation for NSM.

3. Enter the serial number and authorization code.

   Your serial number is printed on the paper license certificate given to you when you purchased NSM. If you do not have the serial number or the LMS System fails to recognize the serial number, call Juniper Networks Customer Service.
Depending on the package you purchased, Juniper Networks provides an authorization code via e-mail. If you received a paper license certificate, and are managing more than 25 devices, call Juniper Networks Customer Service. The Customer Service will validate your purchase and generate a license key.

4. Enter the installation ID that was generated by the NSM Server.

The LMS system generates a license key file for the SKU recorded. You can choose to download the file or to receive it by email.

5. Save the license key file to your local drive for use during installation.

NOTE: The NSM upgrade to 2007.3 or later release will not proceed without the license key file if NSM manages more than 25 devices.

Generating the License Key for an NSM Appliance Upgrade Installation

To generate the license key file to upgrade an NSM appliance:

1. Log in to the LMS system and select License key generation for NSM.

2. Enter the hardware serial number and authorization code.

   The hardware serial number is located on the back of the NSM appliance chassis.

   Depending on the package you purchased, Juniper Networks provides an authorization code via e-mail. If you received a paper license certificate, and are managing more than 25 devices, call Juniper Networks Customer Service. Customer Service will validate your purchase and generate a license key.

   The LMS system generates a license key file for the SKU recorded. You can choose to download the file or to receive it by email.

3. Save the license key file to your local drive for use during installation.

   NOTE: The NSM Xpress upgrade to 2007.3 or later release will not proceed without the license key file if NSM manages more than 25 devices.

Generating the License Key File for an NSM 2007.3 or Later High Availability Upgrade Installation

To generate the license key file to upgrade to NSM 2007.3 or later release with high availability:

1. Run the NSM installer image on the server designated as your primary NSM (or primary GUI Server). The NSM Server generates an installation ID.

2. Run the NSM 2007.3 or later installer image on the server designated as your secondary NSM (or secondary GUI Server). The NSM Server generates an installation ID.

3. Log in to the LMS system and select License key generation for NSM.
4. Enter the serial number and authorization code of your primary NSM.

   For an NSM appliance installation, enter the serial number of the primary server. The 
   hardware serial number is located on the back of the NSM appliance chassis.

   For a software-only installation:
   a. Enter the serial number.

      The serial number of your software is printed on the paper license certificate given 
      to you when you purchased NSM. If you do not have the software serial number or 
      the LMS System fails to recognize the serial number, call Juniper Networks Customer 
      Service.

   b. Enter the installation ID of the primary NSM.

      Depending on the package you purchased, Juniper Networks provides an authorization 
      code via e-mail. If you received a paper license certificate, and are managing more 
      than 25 devices, call Juniper Networks Customer Service. Customer Service will validate 
      your purchase and generate a license key.

5. Select the Need High Availability Key check box. The LMS systems prompts you to 
   provide the NSM Secondary serial number and Secondary Installation ID.

   The LMS system generates a license key file for the SKU recorded. You can choose 
   to download the file, or to receive it by email.

6. Save the license key file to your local drive for use during installation.

   NOTE: The NSM upgrade to 2007.3 or later release will not proceed without 
   the license key file if NSM manages more than 25 devices.

---

**Example of an NSM License File**

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

NSM License File (v1)
Generated on Thu Sep 20 19:11:08 IST 2007

This license file is for:
Serial Number: 00000000 Installation ID: 200003AC65C52
Serial Number: 00000 Installation ID: ID-2

This license file enables the following features:
High-Availability: Enabled
Max-Device: 100
Evaluation-Mode: P30D

This license file reflects the following SKUs:
NS-SM-ADD-50
NS-SM-ADD-50

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.6 (GNU/Linux)
```
NOTE: If your downloaded license key file has any extra lines before "-----BEGIN PGP SIGNED MESSAGE-----" or after "-----END PGP SIGNATURE-----", delete those lines before installing the license key file.

Installing the License Key File in Various Configurations

Instructions for installing the licence key are included in the various installation chapters.

Upgrading the License Key

License upgrades can be purchased at any time for any supported product. After purchasing a license upgrade, you receive a Right to Use (RTU) certificate containing an authorization code that allows you to log into the LMS system and generate a permanent license key that can be applied to the NSM product.

Viewing License Key Information

You can view key information about licenses, in the NSM License Information window. From the menu bar, select Tools > NSM License Information to view this information

Enforcing Licenses

The maximum number of devices allowed for NSMXpress appliance installations is 525. The maximum number of devices allowed for NSM software-only installations is 6025. These numbers include all modeled devices, vsys devices, and cluster devices.

NOTE: Each cluster member of a cluster device counts as one device.

Even though the SKU installation is cumulative, NSM restricts the maximum number of manageable devices. NSM rejects the application for a license when the maximum device supported limit is reached for both appliance and software installations.

If you add a device after the number of devices added reaches 90 percent of the license limit, a warning message appears. If you try to add an extra device after the maximum limit is reached, a dialog box appears with the message “Maximum number of supported devices is reached.” You are not allowed to add devices after reaching the license limit. You must purchase an upgrade before adding more devices.
# Licensing FAQ

Table 9 on page 19 answers frequently asked questions about NSM licensing.

## Table 9: Licensing FAQ

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which device types does NSM count towards the total device count?</td>
<td>NSM counts each single addition of a firewall, IDP, router, switch, Secure Access, or Infranet Controller device as one device. Each cluster member counts as one device. Each vsys device added to a firewall root device counts as one device.</td>
</tr>
<tr>
<td>Does NSM Central Manager (NS-SM-A-CM) require a license key file?</td>
<td>NSM Central Manager does not require a license key file for installation. Enforcement is built into the product.</td>
</tr>
<tr>
<td>Are there any differences in licenses for an NSM appliance and software-only installations?</td>
<td>No. Both follow the same licensing scheme, but their installation methods are different. NSM software version uses NSM Installer to install the new license. An NSM appliance uses the Web UI to install the license. A license can also be installed via the NSM UI after the base installation is completed.</td>
</tr>
<tr>
<td>What is the procedure to add a new license after the device count limit is reached?</td>
<td>License upgrades can be purchased at any time for any supported product. After purchasing a license upgrade, you receive a Right to Use (RTU) certificate containing an authorization code that allows you to log into the LMS system and generate a permanent license key that can be applied to the NSM product. License key updates can then be applied from NSM GUI from Tools &gt; NSM License Information.</td>
</tr>
<tr>
<td>I already have NSM installed in my network. I have &gt;25 devices installed on NSM. Do I need a license key file to upgrade to 2007.3 or later release?</td>
<td>Yes, if you are upgrading from a release that is older than 2007.3.</td>
</tr>
<tr>
<td>What is the procedure to obtain the license key file?</td>
<td>For new installations, see “Installing NSM for the First Time” on page 13. For upgrades, see “Upgrading to an NSM Release that Requires a License” on page 15.</td>
</tr>
<tr>
<td>I don’t have NSM Serial number available. What do I do?</td>
<td>Call Juniper Networks Customer Service.</td>
</tr>
</tbody>
</table>

Copyright © 2011, Juniper Networks, Inc.
CHAPTER 3

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.

This chapter contains the following sections:

• Suggested Standalone Configuration Installation Order on page 21
• Defining System Parameters on page 22
• Prerequisite Steps on page 24
• Installing NSM 2009.1 on page 29
• Installing the User Interface on page 40
• 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 NSM installation CD, or 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 licence. Obtain a license from the Juniper License Management Server (LMS) if you will be managing more and 25 devices (see “Generating the NSM License Key File” on page 13).
   • 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 10 on page 22 identifies the system parameters that you need to identify.

**Table 10: Common System Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
</table>
| Device Server data directory | 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. | By default, the Device Server stores data in: 
/var/netscreen/DevSvr/ |

**CAUTION:** Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.
### Table 10: Common System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI Server data directory</td>
<td>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. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/</td>
<td></td>
</tr>
<tr>
<td><strong>CAUTION:</strong> Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GUI Server database log directory</td>
<td>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. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/xdb/log</td>
<td></td>
</tr>
<tr>
<td>Management IP address</td>
<td>The IP address used by the running GUI Server. The default is the IP address of the machine that you are installing on.</td>
<td></td>
</tr>
<tr>
<td>https port</td>
<td>The port number for listening for messages from the NSM API. The range is from 1025 through 65535. The default value is 8443.</td>
<td></td>
</tr>
<tr>
<td>Initial “super” user password</td>
<td>The password required to authenticate the initial user in the system. By default, the initial superuser account receives all administrative privileges in the system.</td>
<td></td>
</tr>
<tr>
<td>One-time GUI Server password</td>
<td>A password that authenticates the server to its peers in a high-availability configuration, or authenticates a regional server with a central manager.</td>
<td></td>
</tr>
<tr>
<td>Configuration file management</td>
<td>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.</td>
<td>password</td>
</tr>
</tbody>
</table>
### Table 10: Common System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local database backup directory</td>
<td>Directory location where local database backup data is stored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server stores local database backup data at:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/var/netscreen/dbbackup/</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default path is:</td>
<td>/usr/bin/rsync</td>
</tr>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server performs the daily backup within an hour after 2 AM.</td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server stores seven backup files.</td>
<td></td>
</tr>
<tr>
<td>Rsync Backup Timeout</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Enable logging related to local backup and HA.</td>
<td></td>
</tr>
<tr>
<td>Device Server Database Parameters</td>
<td>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”.</td>
<td></td>
</tr>
</tbody>
</table>

### Prerequisite Steps

Before you install the management system, you need to perform the following prerequisite steps:
1. Ensure that the computer you install the management system on is connected to a serial console or monitor and keyboard.

2. Log into the computer 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 computer.

   **NOTE:** Although the management system runs with NSM user permissions, you must have root user permissions to run the 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 (`/var/netscreen` directory).
   
   See “Hardware Recommendations” on page 201 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 installer properly. See “Running the System Update Utility” on page 25 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 26 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 27 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 28 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 “Generating the NSM License Key File” on page 13.

**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 CD 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:
   
   ```bash
gzip -d nsm2009.1r1-systemupdate-linuxES_5.tar.gz
   ```

3. Uncompress the appropriate system update utility .tar file. For example:
   
   ```bash
tar xfv nsm2009.1r1-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:

   ```bash
   <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 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 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`:

```bash
set shmsys:shminfo_shmmax=402653184
set shmsys:shminfo_shmmin=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_semmns=32
```

On Linux systems, you can do this by adding/updating the following line in `/etc/sysctl.conf`:
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:
   ```bash
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
   ```
   If prompted to enter a pass phrase, leave the value blank.

2. Run the following commands on the remote machine:
   ```bash
cd /home/nsm
su nsm
ssh-keygen -t rsa
chmod 0700 .ssh
   ```
   If prompted to enter a pass phrase, 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:
   ```bash
   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:
   ```bash
   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:
   ```bash
   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.

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.

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.ISO8859-1
   en_CA.UTF-8
   en_US
   en_US.ISO8859-1
   en_US.ISO8859-15
   en_US.ISO8859-15@euro
   en_US.UTF-8
   es
   es.UTF-8
   es_MX
   es_MX.ISO8859-1
   es_MX.UTF-8
   fr
   fr.UTF-8
   fr_CA
   fr_CA.ISO8859-1
   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/ProductSUNWladm
   /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
Installing NSM 2009.1

The 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 installer software onto the server where you have decided to use NSM 2009.1. You can run the installer directly from the NSM installation CD, copy the installer to a directory on the server, or download the installer from the Juniper Networks Customer Services online website.

2. Unless installing from CD, navigate to the directory where you saved the management system installer file. We recommend that you save the installer in the /tmp subdirectory.

3. Run the management system installer.

   On Linux, run the following command:
   
   ```bash
   sh nsm2009.1_servers_linux_x86.sh
   ```

   On Solaris, run the following command:
   
   ```bash
   sh nsm2009.1_servers_sol_sparc.sh
   ```

   The installation begins automatically by performing a series of preinstallation checks. The 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 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 installer creates the NSM user, if it does not already exist.

   • For Linux servers, the installer checks whether iptables is running. If not, then the installer continues.
If iptables is running, the 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 installer stops any running servers.

---

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

- "Done" indicates that the installer successfully performed a task.
- "OK" indicates that the installer performed a check and verified that the condition was satisfied.
- "FAILED" indicates that the 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 /tmp.

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

```
[root@/h ~]# sh nsm2009.1_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
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 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 “Generating the NSM License Key File” on page 13 for information about obtaining license keys.

6. The 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 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 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: 3FFEA90278AA

   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 “Generating the License Key for an NSM Software-Only Installation” on page 14.

   b. Enter the license key file path.

      The installer validates the license key file.
NOTE: If the license key file is not there, press Ctrl+Z to exit the installer.
If the NSM Server stops while doing this, you need to manually start the server.

The 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 71, and follow the instructions there.

The 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.
   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, the installer prompts you to try again.

The 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 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 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 into 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 into 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 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, the 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 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 cannot be saved in plain text format, the 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 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 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, the 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, the 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 27

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 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, the installer prompts you for a password. Enter the password again for verification.

The 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 installer will start the server processes with NSM user permissions.

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

The installer prompts you to verify your installation configuration settings.

21. Verify your settings. If they are correct, enter y to proceed. If you enter n, the installer returns you to the original selection prompt.

The 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 the installer on December 1, 2003 at 6:00 PM, the installation log file would be named:

```
netmgtInstallLog.20031201180000
```

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

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

The 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 nsm2009.1_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/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 [10.157.48.108]>

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:
Re type new UNIX password:
password: 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

############ 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/xdb/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

Copyright © 2011, Juniper Networks, Inc.
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
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:
  You will need this for verification purposes when logging into the GUI
  Server. Please make a note of it.

Starting Server Processes Manually

If you did not specify the 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.
Installing the User Interface

The NSM User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based computer 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 computer 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 NSM installation CD or from the Juniper Networks corporate web site to the computer where you are installing the UI.

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

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

   ```bash
   sh nsm2009.1_ui_linux_x86.bin
   ```

   An Introduction screen for the InstallAnywhere wizard appears similar to Figure 1 on page 41.
Chapter 3: Installing NSM in a Standalone Configuration

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

NOTE: If you are installing on a Windows-based computer, then the installer saves the UI software files in C:\Program Files\Network and Security Manager by default. If you are installing on a Linux-based computer, then the 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.
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 computer, 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.
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 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\n
For Linux-based computers:
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 user name, and password. The default user name for new installations is "super"; the default password is the password you specified when configuring the management system. Passwords and user names are case sensitive.

To log into 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 computer, 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 user name 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.

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 Administrate 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 user name 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 4

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 62
• Installing the Device Server on page 63
• Starting Server Processes Manually on page 69
• Validating Management System Status on page 69
• Next Steps on page 69

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 installation CD or the Juniper Networks corporate web site.
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 licence. Obtain a license from the Juniper License Management Server (LMS) if you will be managing more and 25 devices (see “Generating the NSM License Key File” on page 13)
   • 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 11 on page 50 identifies the system parameters that you need to identify.

#### Table 11: Distributed Configuration — System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>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. By default, the Device Server stores data in: <code>/var/netscreen/DevSvr/</code></td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION:** Do not place your data directory in `/usr/netscreen`. That path normally contains binary files and should not be used for data.
Table 11: Distributed Configuration — System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
</table>
| GUI Server data directory        | 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. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/  
CAUTION: Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.                                                                                                                                                                                                                                                                                                                                 |            |
| GUI Server database log directory| 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. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/xdb/log                                                                                                                                                                                                 |            |
| Management IP address            | The IP address and port used by the running GUI Server. The default is the IP address of the machine that you are installing on.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |
### Table 11: Distributed Configuration — System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Database Backup directory</td>
<td>Directory location where local database backup data is stored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server stores local database backup data at:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/var/netscreen/dbbackup/</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable file</td>
<td>Path to the rsync utility executable file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default path is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/usr/bin/rsync</td>
<td></td>
</tr>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server performs the daily backup within an hour after 2 AM.</td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server stores seven backup files.</td>
<td></td>
</tr>
<tr>
<td>Rsync Backup Timeout</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Enable logging related to local backup and HA.</td>
<td></td>
</tr>
<tr>
<td>Device Server Database Parameters</td>
<td>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”.</td>
<td></td>
</tr>
<tr>
<td>Device Server ID</td>
<td>Unique ID assigned when you add the Device Server.</td>
<td></td>
</tr>
<tr>
<td>Password for GUI Server Connection</td>
<td>Password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.</td>
<td></td>
</tr>
</tbody>
</table>
Prerequisites

Perform the prerequisite steps described as if you were installing the management system on the same server. See “Prerequisite Steps” on page 24 for more information.

Installing the GUI Server

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

To install the GUI Server:

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

   On Linux, run the following command:
   
   `sh nsm2009.1_servers_linux_x86.sh`

   On Solaris, run the following command:
   
   `sh nsm2009.1_servers_sol_sparc.sh`

The installation performs a series of preinstallation 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, the 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 installer creates the NSM user, if it does not already exist.

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

If iptables is running, the 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 installer stops any running servers.

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

- "Done" indicates that the installer successfully performed a task.
- "OK" indicates that the installer performed a check and verified that the condition was satisfied.
- "FAILED" indicates that the 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 /tmp.

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

[root@/h ~]# sh nsm2009.1_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 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 licence file path later. See “Generating the NSM License Key File” on page 13 for information about obtaining license keys.

5. The 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 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 installer displays the installation ID of the system prompts you to enter the license key file path.

The installation ID for this system is: 3FFEA90278AA

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 “Generating the License Key for an NSM Software-Only Installation” on page 14.

b. Enter the license key file path.

NOTE: The installer validates the license key file.

If the license key file is not there, press Ctrl+Z to exit the installer. If the NSM Server stops while doing this, you need to manually start the server.
The 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 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 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/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, the installer prompts you to try again.

   The 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 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 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 into 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 into 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 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 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 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 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 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 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 of you want to specify remote backup.

   If you specify that you want the NSM to perform backups, the 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 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 27.

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 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 installer has completed the installation process, enter y. The 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 installer prompts you to verify your installation configuration settings.

16. Verify your settings. If they are correct, enter y to proceed. If you enter n, the installer returns you to the original selection prompt.

The installation proceeds automatically. The 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 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 installer on December 1, 2003 at 6:00 PM, the installation log file would be named `netmgtInstallLog.20031201180000`.

**NOTE:** After the installation script 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 nsm2009.1_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/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 [10.157.48.108]> 

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
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:
  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 40 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 Adminstrate 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. 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)

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

**NOTE:** Before installing the Device Server, verify that the GUI Server is running. After you install the Device Server, the 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 installer file.

2. Run the installer.

   On Linux, run the following command:
   
   sh nsm2009.1_servers_linux_x86.sh

   On Solaris, run the following command:
   
   sh nsm2009.1_servers_sol_sparc.sh

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

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

4. Enter y or n. The 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 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 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 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 installer prompts you to enter parameters assigned by the UI to this Device Server.

   b. Type the Device Server ID.

      The 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 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 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 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 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
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 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 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 superuser. If you specify a user that does not already
exist, the installer prompts you to enter a password for the database superuser.
Enter the password again for verification.

The 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 installer has completed the installation process,
enter y. The 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 installer prompts you to verify your installation configuration settings.

13. Verify your settings. If they are correct, enter y to proceed. If you enter n, the installer returns you to the original selection prompt.

If you confirmed your settings, the installation proceeds automatically. The 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 nsm2009.1_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
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'
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
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
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
Running staging directory.................................ok
NOTES:
- Installation log is stored in /usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20080902144922

[root@C73-16 ~]#

Starting Server Processes Manually

If you did not specify the 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 171 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 5

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 71
- Suggested Simple HA Installation Order on page 78
- Suggested Extended HA Installation Order on page 78
- Defining System Parameters on page 79
- Prerequisites on page 84
- Installing NSM 2009.1 on the Primary Server on page 86
- Installing NSM 2009.1 on the Secondary Server on page 95
- Example: Installing NSM in a Simple HA Configuration on page 95
- Installing the User Interface on page 107
- Configuring the HA Cluster in the UI on page 107
- Installing NSM In an Extended HA Configuration on page 110
- Next Steps on page 129

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 1 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 72 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 73

- HA Server on page 73
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 device 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 shutdown; 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 HaSvr 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 85.

**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/utils/haStatus
```

An example of the output is provided below.

```
[root@NSM1 utils]# ./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 12 on page 77 lists and describes utilities that you can use to manage and maintain the HA server. All these utilities are located in `/usr/netscreen/HaSvr/utils`.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>haStatus</td>
<td>Provides statistics on the HA processes.</td>
</tr>
<tr>
<td>replicateDB</td>
<td>Replicates data to the local or secondary server.</td>
</tr>
<tr>
<td>restoreDbFromBackup</td>
<td>Restores the local backup to current configuration.</td>
</tr>
<tr>
<td>validateBinaries</td>
<td>Checks if all binaries are present to run the server in HA.</td>
</tr>
</tbody>
</table>
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 into 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 into 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 HaSvr 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 do not get replicated without the presence of the 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 13 on page 80 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 13: Simple HA Configuration — System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>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. By default, the Device Server stores data in: /var/netscreen/DevSvr/ CAUTION: Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>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. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/ CAUTION: Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</td>
</tr>
<tr>
<td>GUI Server database log directory</td>
<td>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. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/xdb/log</td>
</tr>
<tr>
<td>Management IP address</td>
<td>The IP address and port used by the running GUI Server. The default is the IP address of the machine that you are installing on.</td>
</tr>
<tr>
<td>https port</td>
<td>The port number for listening for messages from the NSM API. The range is from 1025 through 65535. The default value is 8443.</td>
</tr>
<tr>
<td>Initial “super” user password</td>
<td>The password required to authenticate the initial user in the system. By default, the initial superuser account receives all administrative privileges in the system.</td>
</tr>
</tbody>
</table>
### Table 13: Simple HA Configuration — System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-time GUI Server password</td>
<td>A password that authenticates the server to its peers in a high-availability configuration, or authenticates a regional server with a central manager.</td>
<td></td>
</tr>
<tr>
<td>Configuration file management password</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Primary HA Server IP address</td>
<td>IP address of the primary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>Secondary HA Server IP address</td>
<td>IP address of the secondary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>Heartbeat links between primary and secondary machine</td>
<td>Number of heartbeat communication paths between the primary and secondary machine.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Shared password for heartbeat authentication.</td>
<td>This is the password that is required to authenticate heartbeat messages between the primary and secondary HA servers.</td>
<td></td>
</tr>
<tr>
<td>IP Address for Primary machine's heartbeat link</td>
<td>IP address used for heartbeat communications on the primary server machine.</td>
<td></td>
</tr>
<tr>
<td>Port used for heartbeat communication</td>
<td>The port number used for heartbeat communications.</td>
<td>The default port is 7802.</td>
</tr>
<tr>
<td>Heartbeat messages time interval</td>
<td>Time interval (in seconds) between heartbeat messages.</td>
<td>The default is 15 seconds.</td>
</tr>
<tr>
<td>Missing heartbeats before switchover occurs</td>
<td>Number of missing heartbeat messages before automatic switchover to the secondary machine occurs.</td>
<td>The default is 4 messages.</td>
</tr>
<tr>
<td>IP Address outside the HA cluster</td>
<td>Network IP Address used to monitor this server’s network connection.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 13: Simple HA Configuration — System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA directory</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the HA Server stores data at: /var/netscreen/dbbackup/</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable. The default path is: /usr/bin/rsync</td>
<td></td>
</tr>
<tr>
<td>Path to the ssh utility executable</td>
<td>Path to the ssh utility executable. The default path is: /usr/bin/ssh</td>
<td></td>
</tr>
<tr>
<td>Remote Backup Machine IP Address</td>
<td>IP address of the machine where remote backups are sent. By default, the installer sets this to the IP address of the secondary HA Server.</td>
<td></td>
</tr>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Rsync Backup Timeout</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Enable logging related to local backup and HA.</td>
<td></td>
</tr>
</tbody>
</table>
Table 13: Simple HA Configuration — System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server Database Parameters</td>
<td>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”.</td>
<td></td>
</tr>
</tbody>
</table>

Extended HA Configuration Parameters

Table 14 on page 83 describes additional system parameters that you need to identify to install HA with the Device Server and GUI Server on separate server machines:

Table 14: Extended HA Configuration — System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server ID</td>
<td>Unique ID assigned when you add the Device Server.</td>
<td></td>
</tr>
<tr>
<td>Password for GUI Server Connection</td>
<td>Password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.</td>
<td></td>
</tr>
</tbody>
</table>

Shared Disk Parameters

If you are using a shared disk partition, the installer prompts you to configure additional information. Table 15 on page 83 identifies the additional system parameters that you need to identify to install HA with access to a shared disk:

Table 15: Shared Disk System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to mount the shared disk partition</td>
<td>The command to mount the shared data partition. The default command is: /bin/mount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to unmount the shared disk partition</td>
<td>The command to unmount the shared data partition. Before configuring this command, you must first verify that you have defined your mounts properly. The default command is: /bin/umount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to check the integrity of the shared data partition</td>
<td>The command to check the integrity on the shared data partition. The default command is: /sbin/fsck</td>
<td></td>
</tr>
<tr>
<td>Directory path for the shared disk</td>
<td>Directory path of the shared disk mount point.</td>
<td></td>
</tr>
</tbody>
</table>
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 21 for more information on installing the management system on the same server.

After you have performed the prerequisite steps in “Prerequisite Steps” on page 24 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 84
- “Verifying That All Required System Binaries Are Available” on page 84
- “Verifying That Clocks Are Synchronized” on page 84
- “Establishing an SSH Trust Relationship” on page 85

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/utils` by default).
2. Run the validation shell archive script. You can do so by running the following command:

   ```bash
   ./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 pass phrase, 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 2009.1 on the Primary Server**

After you have successfully performed all prerequisite steps, you can install NSM 2009.1 on your primary server.

To install the primary server with high availability (HA) configured:

1. Load the installer software onto the server where you want to use NSM. You can run the installer directly from the NSM installation CD, copy the installer to a directory on the server, or download the installer from the Juniper Networks Customer Services Online Web site.

2. Navigate to the directory where you saved the installer file. We recommend that you save the installer in the `/tmp` subdirectory.

3. Run the management system installer.

   On Linux, run the following command:
   
   sh nsm2009.1_servers_linux_x86.sh
   
   On Solaris, run the following command:
   
   sh nsm2009.1_servers_sol_sparc.sh

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

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

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

If iptables is running, the 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 installer stops any running servers.

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

- "Done" indicates that the installer successfully performed a task.
- "OK" indicates that the installer performed a check and verified that the condition was satisfied.
- "FAILED" indicates that the 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 /tmp.

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

```
[root@/h ~]# sh sh nsm2009.1_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 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 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 licence 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 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 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 “Generating the License Key for a High Availability NSM Installation” on page 14.

   b. Enter the license key file path.
The installer validates the license key file.

If the license key file is not there, press Ctrl+Z to exit the installer. If the NSM Server stops while doing this, you need to manually start the server.

The 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 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 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 installer prompts you to enter additional parameters required to mount and unmount the partition. Refer to “Shared Disk Parameters” on page 83 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 installer prompts you to try again.

The 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 installer prompts you to enter additional parameters required to mount and unmount the partition. Refer to “Shared Disk Parameters” on page 83 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 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 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 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 into 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 into 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 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 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 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 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 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 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 85, and then restart the installer.

The 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 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 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 27.

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 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 installer prompts you for a password. Enter the password again for verification.

The installer prompts you to start the HA processes when installation is complete.

19. If you want to start the HA processes, enter y.

   The installer will start all processes with nsm user permissions.

20. Verify your settings. If they are correct, enter y to proceed. If you enter n, the installer returns you to the original selection prompt.

   The 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 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 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 installer on December 1, 2003 at 6:00 PM, then the installation log file would be named:

netmgtInstallLog.20031201180000

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

Starting Server Processes Manually

If you did not specify the 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/utils/haStatus
```

The haStatus utility provides additional information describing the state and status of the local/peer servers.

**Other Useful Commands**

Table 16 on page 94 describes some useful commands which may assist in the installation and troubleshooting of your high availability configuration:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>less &lt;filename&gt;</td>
<td>Displays the contents of a text file. The up and down keys can be used to scroll. The letter q to quit.</td>
</tr>
<tr>
<td>netstat -n</td>
<td>Displays the current network connections without resolving any addresses</td>
</tr>
<tr>
<td>while sleep 1;do netstat -n grep 192.168.0.0;done</td>
<td>Continually displays the command after the word “do.” This command is useful if you are waiting for a server connection attempt of data sync.</td>
</tr>
<tr>
<td>clear</td>
<td>Clears the screen</td>
</tr>
</tbody>
</table>
Table 16: Useful Installation and Troubleshooting Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmstat 1</td>
<td>Gives a continuous output of system resource information. The figures at the end of the line give CPU statistics.</td>
</tr>
</tbody>
</table>

Installing NSM 2009.1 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 installer script 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 96 shows this configuration.
The following example shows the complete installer script output for installing the primary GUI Server and Device Server on the same server computer using the configuration described:

```
[root@/h ~]# sh nsm2009.1_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/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 [10.150.41.9]
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)
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]>

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/xdb/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 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
Converting GuiSvr SetDB to XDB .............................ok
Loading GuiSvr XDB data from init files ....................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:  
  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 script output for installing the secondary GUI Server and Device Server on the same server computer using the configuration described:

[root@/h ~]# sh nsm2009.1_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]>

Is this machine the primary server for the HA cluster? (y/n) [y]>

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
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]>
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]> 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]>

Copyright © 2011, Juniper Networks, Inc.
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/xdb/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  
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/netmgInstallLog.20080902154907
- This is the GUI Server fingerprint:
  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 40. 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 Password for GUI Server Connection box, enter the password you specified for
   the “super” user account, when you installed the GUI Server.
5. 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.
6. 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)
7. Click OK to save your settings.

To configure the GUI Server Cluster:
1. From the NSM UI, select Server Manager>Servers>GUIServer, 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 108:
   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 109:
   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

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 110:
   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**

![Image of the New Add/Edit E-mail Address window]

---

**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 83 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 83.
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 112 depicts the configuration example above:
The 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 nsm2009.1_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/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 [10.150.41.9]>
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 database log in /var/netscreen/GuiSvr 
- 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 

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:
  You will need this for verification purposes when logging into the GUI Server. Please make a note of it.
Secondary GUI Server Installation

The following example shows the complete installer script output for installing the secondary GUI Server:

[root@/h ~]# sh nsm2009.1_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..........................

########## 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]>

Is this machine the primary server for the HA cluster? (y/n) [y]>

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/xdb/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:
  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 nsm2009.1_servers_linux_x86.sh

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

Copyright © 2011, Juniper Networks, Inc.
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]>

Copyright © 2011, Juniper Networks, Inc. 123
Enter number of database backups to keep [7]> 7
Enter the rsync backup timeout [3600]> 3600

########## DEVSVR DB SETUP DETAILS ##########
Enter Postgres DevSvr Db port [5432]> 5432
Enter Postgres DevSvr Db super user [nsm]> nsm
Enter Postgres DevSvr Db password for user 'nsm'
Enter password (password will not display as you type)> 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]> 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 nsm2009.1_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 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]

########## DEVSRV 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: 10.150.43.7
- 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 6

Upgrading to NSM 2009.1 from an Earlier Version

This chapter describes how to upgrade the management system and User Interface to Network and Security Manager (NSM) 2009.1. Upgrading includes patching the management system, upgrading the User Interface on your Windows or Linux client, and validating that you have upgraded successfully.

This chapter contains the following sections:

• Upgrade Overview on page 131
• Defining System Parameters on page 132
• Prerequisite Steps on page 137
• Upgrading NSM in a Standalone Configuration on page 140
• Upgrading the User Interface on page 149
• Upgrading NSM in a Distributed Configuration on page 150
• Upgrading NSM with HA Enabled on page 151
• Restoring Data if the Upgrade Fails on page 153
• Next Steps on page 154

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 NSM installation CD or the Juniper Networks corporate 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.

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 17 on page 132 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 17: Standalone Configuration—System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>By default, the Device Server stores data in:</td>
</tr>
<tr>
<td></td>
<td>/var/netscreen/DevSvr/</td>
</tr>
<tr>
<td></td>
<td><strong>CAUTION:</strong> Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server stores data in:</td>
</tr>
<tr>
<td></td>
<td>/var/netscreen/GuiSvr/</td>
</tr>
<tr>
<td></td>
<td><strong>CAUTION:</strong> Do not place your data directory in /usr/netscreen. That path normally contains binary files and should not be used for data.</td>
</tr>
</tbody>
</table>
Table 17: Standalone Configuration—System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address</td>
<td>The IP address used by the running GUI Server. The default is the IP address of the machine that you are installing on.</td>
</tr>
<tr>
<td>https port</td>
<td>The port number for listening for messages from the NSM API. The range is from 1025 through 65535. The default value is 8443.</td>
</tr>
<tr>
<td>Initial “super” user password</td>
<td>The password required to authenticate the initial user in the system. By default, the initial superuser account receives all administrative privileges in the system.</td>
</tr>
<tr>
<td>One-time GUI Server password</td>
<td>A password that authenticates the server to its peers in a high-availability configuration, or authenticates a regional server with a central manager.</td>
</tr>
<tr>
<td>Configuration file management password</td>
<td>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.</td>
</tr>
<tr>
<td>Local database backup directory</td>
<td>Directory location where local database backup data is stored. By default, the GUI Server stores local database backup data at: /var/netscreen/dbbackup/</td>
</tr>
<tr>
<td>Path to the rsync utility executable file</td>
<td>Path to the rsync utility executable file. The default path is: /usr/bin/rsync</td>
</tr>
<tr>
<td>Remote Backup Machine IP Address</td>
<td>IP address of the machine where remote backups are sent. By default, the installer sets this to the IP address of the secondary HA Server.</td>
</tr>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>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. By default, the GUI Server performs the daily backup within an hour after 2 AM.</td>
</tr>
</tbody>
</table>
Table 17: Standalone Configuration—System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>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.</td>
<td>By default, the GUI Server stores seven backup files.</td>
</tr>
</tbody>
</table>

Distributed Configuration Parameters

Table 18 on page 134 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 18: Distributed Configuration — System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server ID</td>
<td>Unique ID assigned when you add the Device Server.</td>
<td></td>
</tr>
<tr>
<td>Password for GUI Server Connection</td>
<td>Password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.</td>
<td></td>
</tr>
</tbody>
</table>

HA Configuration Parameters

Table 19 on page 134 describes the system parameters that you need to identify if you are upgrading a standalone configuration of the management system with HA enabled:

Table 19: HA Configuration — System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary HA Server IP address</td>
<td>IP address of the primary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>Secondary HA Server IP address</td>
<td>IP address of the secondary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>HA replications</td>
<td>Time interval with which you want the GUI Server to replicate the database. By default, the GUI Server replicates the database every 60 minutes.</td>
<td></td>
</tr>
<tr>
<td>Heartbeat links between primary and secondary machine</td>
<td>Number of heartbeat communication paths between the primary and secondary machine. By default, only one communication link exists between the primary and secondary machines.</td>
<td></td>
</tr>
</tbody>
</table>
Table 19: HA Configuration — System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared password for heartbeat authentication.</td>
<td>Password that is required to authenticate heartbeat messages between the primary and secondary HA servers.</td>
<td></td>
</tr>
<tr>
<td>IP Address for Primary machine’s heartbeat link</td>
<td>IP address used for heartbeat communications on the primary server machine.</td>
<td></td>
</tr>
<tr>
<td>Port used for heartbeat communication</td>
<td>The port number used for heartbeat communications. The default port is 7802.</td>
<td></td>
</tr>
<tr>
<td>Heartbeat messages time interval</td>
<td>Time interval (in seconds) between heartbeat messages. The default is 15 seconds.</td>
<td></td>
</tr>
<tr>
<td>Missing heartbeats before switchover occurs</td>
<td>Number of missing heartbeat messages before automatic switchover to the secondary machine occurs. The default is 4 messages.</td>
<td></td>
</tr>
<tr>
<td>IP Address outside the HA cluster</td>
<td>Network IP Address used to monitor this server’s network connection.</td>
<td></td>
</tr>
<tr>
<td>HA directory</td>
<td>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/</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable. The default path is: /usr/bin/</td>
<td></td>
</tr>
<tr>
<td>Remote Backup Machine IP Address</td>
<td>IP address of the machine where remote backups are sent. By default, the installer sets this to the IP address of the secondary HA Server.</td>
<td></td>
</tr>
</tbody>
</table>
Table 19: HA Configuration — System Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>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. By default, the GUI Server performs the daily backup within an hour after 2 AM.</td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server stores seven backup files.</td>
<td></td>
</tr>
</tbody>
</table>

Shared Disk Parameters

Table 20 on page 136 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 20: Shared Disk Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to mount the shared disk partition</td>
<td>The command to mount the shared data partition. The command to unmount the shared data partition. Before configuring this command, you must first verify that your mounts are defined properly. The default command is: /bin/mount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to unmount the shared disk partition</td>
<td>The command to mount the shared data partition. The command to unmount the shared data partition. Before configuring this command, you must first verify that your mounts are defined properly. The default command is: /bin/umount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to check the integrity of the shared data partition</td>
<td>The command to check the integrity on the shared data partition. The default command is: /sbin/fsck</td>
<td></td>
</tr>
<tr>
<td>Directory path of the shared disk</td>
<td>Directory path of the shared disk mount point.</td>
<td></td>
</tr>
</tbody>
</table>
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 installer stops with errors if ScreenOS 4.0.x devices are present in the NSM database.

2. Ensure that the computer you install the management system on is connected to a serial console or monitor and keyboard.

3. Log into the computer 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 computer.

   **NOTE:** Although the management system runs with nsm user permissions, you must have root permissions to run the 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 (`/var/netscreen` directory).

   See "Hardware Recommendations" on page 201 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 178 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 installer properly. See “Running the System Update Utility” on page 138 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 138 for more information.

8. Increase the rsync backup timeout and rsync replication timeout values to 3600. See “Setting the rsync Timeout Values” on page 139.

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 140 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 2009.1 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 CD or 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 nsm2009.1r1-systemupdate-linuxES_5.tar.gz

3. Uncompress the appropriate system update utility .tar file. For example:
   
   tar xfv nsm2009.1r1-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 rhos4_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_shmmin=1
```
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256
set semsys:seminfo_semmap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semms=512
set semsys:seminfo_semmsl=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 2009.1 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_shmmin=1
   set shmsys:shminfo_shmmni=256
   set shmsys:shminfo_shmseg=256
   set semsys:seminfo_semmap=256
   set semsys:seminfo_semmni=512
   set semsys:seminfo_semms=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.ISO8859-1
   - en_CA.UTF-8
   - en_US
   - en_US.ISO8859-1
   - en_US.ISO8859-15
   - en_US.ISO8859-15@euro
   - en_US.UTF-8
   - es
   - es.UTF-8
   - es_MX
   - es_MX.ISO8859-1
   - es_MX.UTF-8
   - fr
   - fr.UTF-8
   - fr_CA
   - fr_CA.ISO8859-1
   - 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](http://www.sun.com). Mount the DVD (in this example, `/solaris`) and issue the following commands:

   `/usr/sbin/pkgadd -d /solaris/Solaris_10/ProductSUNWladm`
   `/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
   ```


   `/usr/sbin/reboot`

Upgrading NSM in a Standalone Configuration

To upgrade to NSM 2009.1 on a standalone system:
1. Load the installer software onto the server where the NSM management system is currently installed. You can run the installer directly from the NSM installation CD. You can also copy the installer to a directory on the server, or you can download the installer from the Juniper Networks Customer Services Online Web site.

2. Unless installing from CD, navigate to the directory where you saved the management system installer file (typically the /tmp/ subdirectory).

3. Run the management system installer.

   On Linux, run the following command:
   
   \texttt{sh nsm2009.1\_servers\_linux\_x86.sh}
   
   On Solaris, run the following command:
   
   \texttt{sh nsm2009.1\_servers\_sol\_sparc.sh}
   
   The installation begins automatically by performing a series of preinstallation checks. The 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 installer discovers ScreenOS 4.0.x or earlier devices in the network, the 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 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.
   \texttt{chkfontpath}

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

   If iptables is running, the 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 installer stops any running servers.

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

- “Done” indicates that the installer successfully performed a task.
- “OK” indicates that the installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the 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 `/tmp`.

The 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
Noting OS name..............................................ok
Stopping any running servers
```

The 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 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

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 2009.1, or if you enter y in response to the previous prompt, you will be prompted for configuration input.

The 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 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 "Generating the License Key for an NSM Software-Only Upgrade" on page 15.

   b. Enter the license key file path.
The installer validates the license key file.

**NOTE:** If the license key file is not there, press Ctrl+Z to exit the installer. If the NSM Server stops while doing this, you need to manually start the server.

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 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 installer prompts you to verify your upgrade configuration settings.

11. Verify your settings. If they are correct, enter y to proceed. If you enter n, the installer returns you to the original selection prompt.

    The upgrade proceeds automatically. The 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 installer runs for several minutes, and then exits.

After the installer finishes, it generates a log file with the output of the installation commands for troubleshooting purposes. The 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 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 nsm2009.1_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 2009.1r1
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
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
Enabled 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:
  You will need this for verification purposes when logging into the GUI
  Server. Please make a note of it.

[root@C73-16 ~]#

**Starting Server Processes Manually**

If you did not specify the 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 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 171 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 2009.1 Release automatically. For earlier releases, you must manually download and install the new UI client.

- Downloading and Installing the UI Client Automatically on page 149
- Downloading and Installing the UI Client Manually on page 150
- Validating the Upgrade on page 150

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 NSM installation CD or from the Juniper Networks corporate web site, follow the steps described in “Installing the User Interface” on page 40.

The NSM User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based computer 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 149 for details.

6. Launch the UI and verify that you can connect to the upgraded GUI Server.

**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 24. 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 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 installer on the secondary server (if applicable). Configure parameters that are appropriate for the secondary server.

The installer generates an installation ID and prompts you to enter the license key. For information about generating the license key, see “Generating the License Key File for an NSM 2007.3 or Later High Availability Upgrade Installation” on page 16.

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]> 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 license key file is not there, press Ctrl+Z to exit the installer.
If the NSM Server stops while doing this, you need to manually start the server.

7. Enter the license key in the primary server. The 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 149 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 71 for more information.

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 181 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. Check the audit log in the UI for any changes that you might have made after installing NSM. This will provide you with guidelines for any data that you might need to restore.
2. Remove all existing components of the NSM management system. See “Removing the Management System” on page 188 for more information.
3. Perform a clean installation of NSM. Refer to the appropriate version of NSM documentation for more information about installing your version of NSM.
4. Restore your configuration and log data from backup. See “Archiving and Restoring Logs and Configuration Data” on page 178 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.
This chapter describes how to upgrade the management system on an NSM Xpress appliance or NSM Central Manager (NSMCM) appliance to Network and Security Manager (NSM) 2009.1. 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:

- Upgrading NSM Xpress and NSMCM Appliances on page 155
- NSM Xpress Data Migration on page 165
- User Privileges on NSM Xpress on page 169

Upgrading NSM Xpress and NSMCM Appliances

Upgrading to NSM 2009.1 Release on an NSM Appliance

NSM 2009.1 requires a license file if you are managing more than 25 devices. You must have the license file before performing the upgrade to NSM 2009.1. The NSM installer will not proceed without the license file.

For information on the procedure for generating the license file, refer to “Generating the NSM License Key File” on page 13.

Use the following procedure to upgrade to NSM 2009.1 on an NSM Xpress appliance.

1. From the NSM Software Download page, click the Regional Server upgrade link to download the NSM Xpress Appliance software. The downloaded file has the name nsm2009.1r1_servers_upgrade_rs.zip.

2. Copy this file onto your NSM Xpress appliance 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. Confirm that the unzip utility is present on the NSM Xpress 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
```

6. Navigate to the directory where you saved the downloaded file, which is typically the `/tmp/` subdirectory.

7. Enter the following command to unzip and save the two files (`nsm2009.1r1_servers_linux_x86.sh`, `upgrade-os.sh`) and a directory (`apps-rpms`) on the NSMXpress appliance:

```
unzip nsm2009.1r1_servers_upgrade_rs.zip
```

8. Enter the following command to automatically start the installation:

```
sh upgrade-os.sh nsm2009.1r1_servers_linux_x86.sh
```

The installer begins a series of preinstallation 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 installer successfully performed a task.
- "OK" indicates that the installer performed a check and verified that the condition was satisfied.
- "FAILED" indicates that the 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`.

The 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 installer perform a clean install of NSM.
10. The 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 installer prompts to configure these options.

The script 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 script prompts you to verify your upgrade configuration settings.

12. Verify your settings. If they 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 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 postinstallation tasks such as removing the staging directory and starting the server processes (if configured).

Messages display the installation progress.

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting. The 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 installer file `nsm2009.1r1_servers_linux_x86.sh` to the `/var/install` directory and enter the following commands:

```
rm -f NSM-RS
chmod 755 nsm2009.1r1_servers_linux_x86.sh
ln -s nsm2009.1r1_servers_linux_x86.sh NSM-RS
```

---

**Upgrading to NSM 2009.1 Release on an NSM Central Manager Appliance**

---

**NOTE:** NSM 2009.1 for Central Manager does not require a license file.
Use the following procedure to upgrade to NSM 2009.1 on an NSM CM appliance.

1. From the NSM Software Download page, click the **Central Manager upgrade** link to download the NSM Central Manager Appliance software. The downloaded file has the name `nsm2009.1r1_servers_upgrade_cm.zip`.

2. Copy this file onto your NSM CM appliance using FTP or SCP.

3. Log in as the admin user, and answer `n` when prompted to run the setup wizard.

4. Enter `sudo su` - and enter the admin password to gain root access.

5. Confirm that the `unzip` utility is present on the NSM CM appliance by entering the following command:

   ```bash
   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:

   ```bash
   yum install unzip
   ```

6. Navigate to the directory where you saved the downloaded file, which is typically the `/tmp/` subdirectory.

7. Enter the following command to unzip and save the two files (`nsm2009.1r1_servers_cm.sh`, `upgrade-os.sh`) and a directory (`apps-rpms`) on the NSM Central Manager system:

   ```bash
   unzip nsm2009.1r1_servers_upgrade_cm.zip
   ```

8. Enter the following command to automatically start the installation.

   ```bash
   sh upgrade-os.sh nsm2009.1r1_servers_cm.sh
   ```

   The installer begins a series of preinstallation 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 installer successfully performed a task.
- “OK” indicates that the installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the 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.

The 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 installer perform a clean install of Central Manager.

10. The 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 installer prompts to configure these options.

The script 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 script prompts you to verify your upgrade configuration settings.

12. Verify your settings. If they are correct, type y and press Enter to proceed. If settings are not correct, or type n and press Enter to return to the original selection prompt.

    The upgrade proceeds automatically. The installer performs the following actions:

    - Extracts and decompresses the software payloads.
    - Upgrades Central Manager.
    - Installs the HA Server.
Sets start scripts.

- Performs postinstallation tasks such as removing the staging directory and starting the server processes (if configured).

Messages display the installation progress.

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting. The 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 installer file `nsm2009.1r1_servers_cm.sh` to the `/var/install` directory and enter the following commands:

   ```
   rm -f NSM-CM
   chmod 755 nsm2009.1r1_servers_cm.sh
   ln -s nsm2009.1r1_servers_linux_cm.sh NSM-CM
   ```

Upgrading to NSM 2009.1 Release on an NSMXpress Appliance (Offline Mode)

The section provides instructions on upgrading to NSM 2009.1 on an NSMXpress appliance if the NSMXpress appliance is not connected to the Internet.

1. From the NSM Software Download page, click the **Regional Server upgrade** link to download the NSMXpress Appliance upgrade software. The downloaded file has the name `nsm2009.1r1_servers_upgrade_rs.zip`.

2. From the NSM Software Download page, click the **Offline Server upgrade** link to download the NSMXpress Appliance offline upgrade software. The downloaded file has the name `nsm2009.1r1_offline_upgrade.zip`.

3. Copy the following files onto your NSMXpress appliance. Download both files to the same location using FTP or SCP.

   ```
   nsm2009.1r1_servers_upgrade_rs.zip
   nsm2009.1r1_offline_upgrade.zip
   ```

4. Log in as the admin user, and answer `n` when prompted to run the setup wizard.

5. Enter the following command, and then enter the admin password to gain root access.

   ```
   sudo su -
   ```

6. Confirm that the `unzip` utility is present on the NSMXpress 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. Navigate to the directory where you saved the downloaded files, which is typically the `/tmp/` subdirectory.
8. Enter the following command to unzip the files (\textit{nsm2009.1r1_servers_linux_x86.sh}, \textit{upgrade-os.sh}) and create a directory (\textit{apps-rpms}) in which NSMXpress saves the unzipped files.

\texttt{unzip nsm2009.1r1_servers_upgrade_rs.zip}

9. Enter the following command to start the installation.

\texttt{sh upgrade-os.sh nsm2009.1r1_servers_linux_x86.sh Offline}

The installer begins a series of preinstallation 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.

\textbf{NOTE:} The management system installer indicates the results of its specific tasks and checks:

- "Done" indicates that the installer successfully performed a task.
- "OK" indicates that the installer performed a check and verified that the condition was satisfied.
- "FAILED" indicates that the 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 \texttt{/usr/netscreen/DevSvr/var/errorLog}. If the failure happens in the early stages of installation, the log might be in \texttt{/tmp}.

The installer then stops any running servers.

10. Type 2 to specify that you want to upgrade both the Device Server and the GUI Server.

\textbf{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 installer perform a clean install of NSM.

11. The 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 installer prompts to configure these options.

The script next prompts you to restart the servers when the installation is finished.

12. 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 script prompts you to verify your upgrade configuration settings.

13. Verify your settings. If they 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 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 postinstallation tasks such as removing the staging directory and starting the server processes (if configured).

Messages display the installation progress.

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting. The 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.

14. After successful installation, copy the installer file nsm2009.1r1_servers_linux_x86.sh to the /var/install directory and enter the following commands:

   rm -f NSM-RS
   chmod 755 nsm2009.1r1_servers_linux_x86.sh
   ln -s nsm2009.1r1_servers_linux_x86.sh NSM-RS

Upgrading to NSM 2009.1 Release on an NSM Central Manager Appliance (Offline Mode)

The section provides instruction on upgrading to NSM 2009.1 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 Central Manager upgrade link to download the NSM Central Manager Appliance software. The downloaded file will have the name nsm2009.1r1_servers_upgrade_cm.zip.

2. From the NSM Software Download page, click the Offline Server upgrade link to download the NSM CM appliance offline upgrade software. The downloaded file will have the name nsm2009.1r1_offline_upgrade.zip.
3. Copy the following files onto your NSM CM appliance using FTP or SCP. Download both files to the same location.
   - nsm2009.1r1_servers_upgrade_cm.zip
   - nsm2009.1r1_offline_upgrade.zip

4. Log in as the admin user, and type `n` when prompted to run the setup wizard.

5. Enter the following command, and then enter the admin password to gain root access.
   ```
   sudo su -
   ```

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.E14.5.i386.rpm
   ```

7. Navigate to the directory where you saved the downloaded files, which is typically the `/tmp/` subdirectory.

8. Enter the following command to unzip and save two files (`nsm2009.1r1_servers_cm.sh`, `upgrade-os.sh`) and a directory (`apps-rpms`) on the NSM Central Manager appliance:
   ```
   unzip nsm2009.1r1_servers_upgrade_cm.zip
   ```

9. Enter the following command to automatically start the installation:
   ```
   sh upgrade-os.sh nsm2009.1r1_servers_cm.sh Offline
   ```
   The installer begins a series of preinstallation 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 installer successfully performed a task.

- “OK” indicates that the installer performed a check and verified that the condition was satisfied.

- “FAILED” indicates that the 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.

The installer then stops any running servers.

10. 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 installer perform a clean install of the Central Manager.

11. The 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 installer prompts to configure these options.

The script next prompts you to restart the servers when the installation is finished.

12. 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 script prompts you to verify your upgrade configuration settings.

13. Verify your settings. If they 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 installer performs the following actions:

- Extracts and decompresses the software payloads.
- Upgrades the Central Manager.
- Installs the HA server.
• Sets start scripts.

• Performs postinstallation tasks such as removing the staging directory and starting the server processes (if configured).

Messages display the installation progress.

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting. The 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.

14. After the successful installation, copy the installer file (`nsm2009.r1_servers_cm.sh`) to the `/var/install` directory and then enter the following commands:

```bash
rm -f NSM-CM
chmod 755 nsm2009.r1_servers_cm.sh
ln -s nsm2009.r1_servers_linux_cm.sh NSM-CM
```

NSMXpress Data Migration

This section provides information on how to port data from a Solaris server or a Linux server running NSM to an NSMXpress appliance. It contains the following procedures:

• Solaris to NSMXpress Data Migration on page 165

• Linux to NSMXpress Data Migration on page 167

Solaris to NSMXpress Data Migration

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 NSMXpress appliance.

2. Stop the NSM processes:

   ```bash
   /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:

   ```bash
   rm -f /tmp/xdbExporter.pid
   ```
4. Use FTP to copy `csvfile.txt` to a common location.

**On the NSMXpress appliance:**

1. Use the `nsm_setup` utility to:
   
   a. Change the IP address, netmask, and gateway of the NSMXpress server to those of the Solaris server, if you need to use the same IP configuration in NSMXpress.

   b. Perform a clean installation of the latest release of NSM on the NSMXpress appliance, or install the same release you installed on the Solaris server.

   ```
   NOTE: The version of NSM on the NSMXpress 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 HaSvr, GuiSvr, and DevSvr processes with the following commands:

   ```
   /usr/netscreen/GuiSvr/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 NSMXpress appliance: Option 70.server.00.server.1

   ```bash
   [nsm@NSMXpress ~]$ /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 devSrv.cfg to match the one-time password in the shadow_server table:
    a. Use the vi editor to edit the /var/netscreen/DevSvr/devSrv.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 devSrv.cfg.

11. Start the HaSvr, GuiSvr, and DevSvr processes by entering the following command:
    /usr/netscreen/HaSvr/bin/haSvr.sh start

Linux to NSMXpress Data Migration

This section describes how to port data from an existing Linux server to NSMXpress. This section makes the following assumptions:

- The IP address of the existing Linux server will be assigned to the new NSMXpress server.
- The versions of NSM are the same on the current Linux installation and the new NSMXpress installation. If the versions are different, you must upgrade the Linux server to the NSM version that is running on NSMXpress 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 NSMXpress 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.

   ```
   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 an NSMXpress Appliance

1. Use the `nsm_setup` utility to:

   a. Change the IP address, netmask, and gateway of the NSMXpress server to those of the Linux server, if you need to use the same IP configuration in NSMXpress.

   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 NSMXpress 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 NSMXpress as you had for the Linux server, follow Step 6, Step 7, and Step 9 of the procedure for migrating data from Solaris to NSMXpress. See “On the NSMXpress appliance:” on page 166.

   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 NSMXpress, follow Step 6, Step 8, Step 9, and Step 10 of the procedure for migrating data from Solaris to NSMXpress. See “On the NSMXpress appliance:” on page 166.

   These steps are required:
   - To delete the existing RSA keys between devSvr and guiSvr from the devSvr.cfg file so they can be renegotiated and established again.
   - To 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 HaSvr, GuiSvr, and DevSvr processes:
   ```
   /usr/netscreen/HaSvr/bin/haSvr.sh start
   ```

**User Privileges on NSMXpress**

NSMXpress 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]
   ```
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 171
- Configuring Server Options on page 173
- Archiving and Restoring Logs and Configuration Data on page 178
- Configuring High Availability Options on page 180
- Relocating the Database on page 183
- Installing a Trivial File Transfer Protocol Server on page 185
- Modifying Timeout Values on the Device Server on page 187
- Downgrade Procedures on page 188
- Removing the Management System on page 188
- Uninstalling the User Interface on page 190

### 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:
   ```bash
   cd /usr/netscreen/GuiSvr/bin
   ```
2. Run the following command:
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 21 on page 172 describes the commands that the management system supports.

**Table 21: Management System Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Sends a hangup signal to the management system process, and then instructs the process to reload its configuration and start again.</td>
</tr>
<tr>
<td>restart</td>
<td>Stops the management system process for two seconds, and then restarts the process.</td>
</tr>
<tr>
<td>start</td>
<td>Starts the management system process.</td>
</tr>
<tr>
<td>stop</td>
<td>Stops the management system process.</td>
</tr>
<tr>
<td>status</td>
<td>Provides a status of the management system process.</td>
</tr>
<tr>
<td>version</td>
<td>Lists the current version of the management system.</td>
</tr>
</tbody>
</table>

### 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 HaSvr 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 174
- Changing the Device Server IP Address on page 174
- Changing the GUI Server IP Address on page 175
- Configuring Disk Space Management on the Device Server on page 175
- Configuring Disk Space Management on the GUI Server on page 176
- Configuring Connection Timing on page 177
- Setting Core File Naming on Solaris on page 177
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.
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.
7. Navigate to the utils directory. Run the `.xdbUpdate` utility to update the IP Address. Run the following:
   ```bash
   export LD_LIBRARY_PATH=/usr/netscreen/GuiSvr/utils/dbxml-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:
   ```bash
   export LD_LIBRARY_PATH=/usr/netscreen/GuiSvr/utils/dbxml-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:
   ```bash
   export LD_LIBRARY_PATH=/usr/netscreen/GuiSvr/utils/dbxml-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.
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 an alert.
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 check 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 GUI 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 computer as root.

2. Run the following command:

   ```bash
   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.
   ```
   ls -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.
   ```
   ls -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 backup 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 <hostname>
b
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/GuiSvr or /usr/netscreen/DevSvr). It is not recommended that you have these links point to locations that are inside /usr/netscreen/GuiSvr or /usr/netscreen/DevSvr. 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 (haSvr.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/utils` by default).
3. Run the replicate database shell archive script. You can do so by running the following command as nsm user:
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/utils` 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:

   ```bash
   restoreDbFromBackup.sh N
   ```

   For example, to restore the backup file from Friday:

   ```bash
   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.
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 21 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
   8507CCD5E0E1B08F270020E8027 EEC23CC60D454B01A75642FE28
   DCA4B165E808DD90FE0D933CA3
   65CFA11001250020 E1BD3D38C8E287B9D5DBC6B76865
   F12E28C3A1736B30CBD7A98A9721DFB97E7)

   :theirRsaPublicKey
   (0020CBCE9B75418130C8805A3EDD7E21C6775FEAFCD92155F0E2
   101EA2A4B06F0B2500125)

f. Save and exit from the 0.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 0.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
}
```
4. 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:

1. Open the `/etc/inetd.conf` file in any text editor.
2. Uncomment the line that begins with “tftp” or “#tftp”.

```
3. 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
```

4. Restart the inetd service. You can do so by running the following commands:

```
/etc/init.d/inetsvc stop
/etc/init.d/inetsvc 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:

1. 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
     ```

2. 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
   ```
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 188 for more information.
3. Install your previous version of NSM.
4. Restore your backup database. See “Restoring the Database” on page 182 for more information.

Removing the Management System

To remove previous management system installations:
1. Stop the HA Server by entering the following command:
   
   ```bash
   /usr/netscreen/HaSvr/bin/haSvr.sh stop
   ```
2. Stop the Device Server by entering the following command:
   
   ```bash
   /usr/netscreen/DevSvr/bin/devSvr.sh stop
   ```
3. Stop the GUI Server by entering the following commands:
   
   ```bash
   /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.
      
      ```bash
      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 NSCNguiisv 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.
   ## Removing pathnames in class <none>
   /usr/netscreen/DevSvr/utils/policy_compiler
   /usr/netscreen/DevSvr/utils/nacnUpdateCA
   /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
cdl/init.d root# ls *Svr
devSvr guiSvr haSvr
cdl/init.d root# rm -f *Svr
cdl/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 computer, 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 computer, use the Start menu, then select Network and Security Manager > Uninstall Network and Security Manager.

   On a Linux-based computer, 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 193
• Hardware Recommendations on page 201
• Profiler Performance Tuning Recommendations on page 209
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 12 on page 193:

- Management system
- User interface (UI)
- Managed devices

**Figure 12: NSM Architecture**

This appendix contains the following sections:

- About the Management System on page 194
- About the NSM User Interface on page 195
- About Managed Devices on page 195
- Server Communications on page 195
- Using the Secure Server Protocol on page 197
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 13 on page 194 shows these components.

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 20 UI clients connected to it at any time. 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 6000 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


The following tables list the inbound and outbound ports on the NSM management system.

### Table 22: Inbound ports on the NSM Management System

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>In an HA setup, the HA server synchronizes the Primary and Secondary NSM servers using rsync to transfer files through this port.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>The client computer accesses the NSMxpress Web interface using this port.</td>
</tr>
<tr>
<td>5432</td>
<td>TCP</td>
<td>STRM devices connect to the PostgreSQL on this port to get profiler data.</td>
</tr>
<tr>
<td>7800</td>
<td>TCP</td>
<td>Devices running ScreenOS Software connect to the Device Server on this port.</td>
</tr>
</tbody>
</table>
| 7801 | TCP      | • 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 Software, 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 23: Outbound ports on the NSM Management System**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP</td>
<td>The port used to upload output to Juniper FTP when requesting technical support.</td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>In an <strong>IP reachable</strong> workflow, the Device Server uses this port to send commands to the device using SSH (a one-time connection).</td>
</tr>
<tr>
<td>23</td>
<td>TCP</td>
<td>In an <strong>IP reachable</strong> workflow, the Device Server uses this port to send commands to the device using Telnet (a one-time connection).</td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>If configured to send e-mail alerts, the Device Server (SNMP client) connects to the SMTP server on this port.</td>
</tr>
<tr>
<td>53</td>
<td>UDP</td>
<td>During an attack database download, the Domain Name System (DNS) client resolves addresses using this port.</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>If Network Time Protocol (NTP) is used for clock synchronization, the Device Server connects to the NTP server on this port.</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>The NSM Topology Discovery Manager uses SNMP to communicate with devices through this port.</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>The Device Server sends SNMP traps to servers that listen on this port.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>The Device Server downloads the attack database and the Device Management Interface (DMI) schema using this port.</td>
</tr>
<tr>
<td>514</td>
<td>UDP</td>
<td>If configured, the Device Server forwards logs in Syslog format to this port.</td>
</tr>
<tr>
<td>1645</td>
<td>UDP</td>
<td>If configured, the Device Server connects to the RADIUS authentication server on this port.</td>
</tr>
<tr>
<td>1646</td>
<td>UDP</td>
<td>If configured, the Device Server connects to the RADIUS accounting server using this port.</td>
</tr>
<tr>
<td>7801</td>
<td>TCP</td>
<td>The Device Server communicates with the GUI Server on this port.</td>
</tr>
<tr>
<td>9020</td>
<td>UDP</td>
<td>If configured through NSM, a firewall uses this port for integrated surf control for Web filtering.</td>
</tr>
</tbody>
</table>

**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 24 on page 198 lists and describes the ports used specifically in communications
between NSM and ScreenOS 5.0 devices.

Table 24: Management System Communications With Devices Running
ScreenOS

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 7800</td>
<td>Accepts incoming connections from devices running ScreenOS 5.0 and later.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 7801</td>
<td>Communicates with the GUI Server.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 22/23</td>
<td>SSH/Telnet to import initial configurations of devices running ScreenOS 5.0 and later.</td>
</tr>
<tr>
<td>GUI Server</td>
<td>Inbound TCP: 7808</td>
<td>Accepts communication from the GUI client.</td>
</tr>
</tbody>
</table>

**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 25 on page 199 lists and describes the ports used specifically in communications between NSM and DMI-compatible devices.

Table 25: Management System Communications With DMI-Compatible Devices

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 7804</td>
<td>Accepts incoming device connections.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 7801</td>
<td>Communicates with the GUI server.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 22/23</td>
<td>SSH/Telnet to import initial configurations of DMI-compatible devices.</td>
</tr>
<tr>
<td>GUI Server</td>
<td>Inbound TCP: 7808</td>
<td>Accepts communication from the GUI client.</td>
</tr>
</tbody>
</table>

**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.
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 201
- Network Card Requirements on page 202
- Memory Requirements on page 202
- Storage Space Requirements on page 204
- Processor Speed Requirements on page 206
- Recommendations for Large-Scale Installations on page 207

**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 26 on page 202 to determine the estimated RAM required:

<table>
<thead>
<tr>
<th>Total Config Size</th>
<th>GUI Server RAM Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 2 MB</td>
<td>2 GB</td>
</tr>
<tr>
<td>Between 2 and 10 MB</td>
<td>3 GB</td>
</tr>
</tbody>
</table>
Appendix B: Hardware Recommendations

Table 26: GUI Server RAM Requirements (continued)

<table>
<thead>
<tr>
<th>Total Config Size</th>
<th>GUI Server RAM Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between 10 and 50 MB</td>
<td>4 GB</td>
</tr>
<tr>
<td>More than 50 MB</td>
<td>8 GB</td>
</tr>
</tbody>
</table>

Device Server

The key factor in determining the memory requirements for the Device Server is the number of devices you are managing. Use Table 27 on page 203 to determine the requirements for a given deployment size if the Device Server is managing firewall/VPN devices or JUNOS devices.

Table 27: Device Server RAM Requirements for Firewall/VPN or JUNOS Devices

<table>
<thead>
<tr>
<th>Number of Devices</th>
<th>Device Server RAM Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 200</td>
<td>2 GB</td>
</tr>
<tr>
<td>More than 200</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

Use Table 28 on page 203 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 28: Device Server RAM Requirements for IDP, Secure Access, or Infranet Controller Devices

<table>
<thead>
<tr>
<th>Number of Devices</th>
<th>Device Server RAM Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 through 3</td>
<td>2 GB</td>
</tr>
<tr>
<td>4 through 8</td>
<td>4 GB</td>
</tr>
<tr>
<td>9 through 30</td>
<td>8 GB</td>
</tr>
</tbody>
</table>

UI Client

For managing a network with at least one DMI-compatible device in it, we recommend a minimum of 1 GB of RAM. For managing only ScreenOS and IDP devices, we recommend a minimum of 512 MB of RAM, or 1 GB if you have 1000 or more ScreenOS and IDP devices in your network. 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:

Change:

lax.nl.java.option.java.heap.size.max=384m
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 29 on page 204.

Table 29: Audit Log Details

<table>
<thead>
<tr>
<th>Operation</th>
<th>Audit Log Detail OFF</th>
<th>Audit Log Detail ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Device 10K</td>
<td>408 bytes</td>
<td>40 KB</td>
</tr>
<tr>
<td>Update Device 30K</td>
<td>408 bytes</td>
<td>60 KB</td>
</tr>
<tr>
<td>Update Device 300K</td>
<td>456 bytes</td>
<td>240 KB</td>
</tr>
<tr>
<td>Add Device</td>
<td>6K</td>
<td>5 KB</td>
</tr>
<tr>
<td>Login in/out</td>
<td>540 bytes</td>
<td>180 bytes</td>
</tr>
</tbody>
</table>
Table 29: Audit Log Details (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Audit Log Detail OFF</th>
<th>Audit Log Detail ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save Policy 25 rules</td>
<td>144 bytes</td>
<td>.01 MB</td>
</tr>
<tr>
<td>Save Policy 100 rules</td>
<td>192 bytes</td>
<td>0.5 MB</td>
</tr>
<tr>
<td>Save Policy 250 rules</td>
<td>1536 bytes</td>
<td>0.75 MB</td>
</tr>
<tr>
<td>Save Policy 1000 rules</td>
<td>3072 bytes</td>
<td>5 MB</td>
</tr>
<tr>
<td>Save Policy 5000 rules</td>
<td>6144 bytes</td>
<td>15 MB</td>
</tr>
</tbody>
</table>

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:
  \[100 \times 40 \text{ KB} + 5 \times 5 \text{ MB} = 29 \text{ MB}\] of disk space

- With the audit log details turned off, the audit log uses only:
  \[100 \times 408 \text{ bytes} + 5 \times 1 \text{ KB} = 45 \text{ KB}\] of disk space.

The GUI Server also requires 2 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:

\[(10 \text{ KB} \times 100) \times 200 = 200 \text{ MB}\] 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 * (device configuration database size calculated above).

Device Server Requirements

Storage capacity requirements are determined by the following equation:
(Retention period in days * Events per day * 200 bytes) / 1,000,000,000 = storage size in GB.

Log events average around 200 bytes each. Table 30 on page 206 lists some examples for a Device Server managing just firewall/VPN devices based on a retention period of 30 days:

Table 30: Storage Requirements for Device Server Managing Firewall/VPN Devices

<table>
<thead>
<tr>
<th>Events Per Day</th>
<th>Storage required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000,000</td>
<td>6 GB</td>
</tr>
<tr>
<td>10,000,000</td>
<td>60 GB</td>
</tr>
<tr>
<td>25,000,000</td>
<td>150 GB</td>
</tr>
<tr>
<td>50,000,000</td>
<td>300 GB</td>
</tr>
</tbody>
</table>

Table 31 on page 206 lists some examples for a Device Server managing just IDP stand-alone devices running profiler based on a retention period of 30 days:

Table 31: Storage Requirements for Device Server Managing IDP (w/Profiler) Devices

<table>
<thead>
<tr>
<th>Number of Profiling Devices</th>
<th>Storage required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>8 GB</td>
</tr>
<tr>
<td>3 through 8</td>
<td>12 GB</td>
</tr>
<tr>
<td>9 through 20</td>
<td>24 GB</td>
</tr>
</tbody>
</table>

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

A faster CPU supports higher sustained logging rates, improving scalability on the Device Server. A modern Intel or AMD CPU (2.4GHz) or an UltraSparc III (1.2 GHz) can handle sustained log rates of at least 20,000 logs per second.

Device Server Managing IDP Standalone Devices Running Profiler

More CPUs enable the Device Server to manage more IDP standalone devices running profiler. See Table 32 on page 207.

Table 32: CPU Requirements for Device Server Managing IDP (w/Profiler) Devices

<table>
<thead>
<tr>
<th>Number of Profiling Devices</th>
<th>CPUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>1</td>
</tr>
<tr>
<td>3 through 8</td>
<td>2</td>
</tr>
<tr>
<td>9 through 20</td>
<td>4</td>
</tr>
</tbody>
</table>

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.
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 209
- Setting Preferences to Improve Profiler Performance on page 212

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 33 on page 209 describes recommendations for optimum performance when managing one to two profiling devices.

Table 33: Performance Turning Recommendations for Low-End Configurations

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Setup</td>
<td>GUI Server and Device Server (Profiler DB) running on the same machine</td>
<td>N/A</td>
</tr>
<tr>
<td>Physical Memory Required</td>
<td>1 GB</td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>1 Fast</td>
<td></td>
</tr>
<tr>
<td>Disk space reserved for Profiler</td>
<td>8 GB</td>
<td></td>
</tr>
<tr>
<td>UI System Preferences</td>
<td>Purge profiler database if size exceeds</td>
<td>1000 MB</td>
</tr>
</tbody>
</table>
Table 33: Performance Turning Recommendations for Low-End Configurations (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max profiler database size after purging</td>
<td>750 MB</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL Settings</td>
<td>shared_buffers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>for Linux</td>
<td>1000 KB</td>
</tr>
<tr>
<td></td>
<td>for Solaris</td>
<td>700 KB</td>
</tr>
<tr>
<td>work_mem</td>
<td></td>
<td>16384 KB</td>
</tr>
<tr>
<td>maintenance_work_mem</td>
<td></td>
<td>8192 KB</td>
</tr>
<tr>
<td>max_fsm_pages</td>
<td></td>
<td>20000 disk pages</td>
</tr>
<tr>
<td>checkpoint_segments</td>
<td></td>
<td>64 log file segments</td>
</tr>
<tr>
<td>checkpoint_timeout</td>
<td></td>
<td>600 seconds</td>
</tr>
<tr>
<td>Device Server</td>
<td>profilerMgr.receiver.maxParallelConns</td>
<td>Reduce from 3 to 1</td>
</tr>
</tbody>
</table>

See “Setting Preferences to Improve Profiler Performance” on page 212 for more information on recommended settings.

Medium-Size Configuration (3 to 8 IDP Profiling Devices)

Table 34 on page 210 describes recommendations for optimum performance when managing 3 to 8 profiling devices.

Table 34: Performance Turning Recommendations for Medium-Sized Configurations

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Setup</td>
<td>GUI Server and Device Server (Profiler DB) running on the same machine</td>
<td>N/A</td>
</tr>
<tr>
<td>Physical Memory Required</td>
<td></td>
<td>2 GB</td>
</tr>
<tr>
<td>CPU</td>
<td></td>
<td>2 Fast</td>
</tr>
<tr>
<td>Disk space reserved for Profiler.</td>
<td>*High-end SCSI drives preferred</td>
<td>12 GB</td>
</tr>
<tr>
<td>UI System Preferences</td>
<td>Purge profiler database if size exceeds</td>
<td>3000 MB</td>
</tr>
<tr>
<td>Max profiler database size after purging</td>
<td></td>
<td>2200 MB</td>
</tr>
<tr>
<td>PostgreSQL Settings</td>
<td>shared_buffers</td>
<td>32768 KB</td>
</tr>
</tbody>
</table>

Copyright © 2011, Juniper Networks, Inc.
### Table 34: Performance Turning Recommendations for Medium-Sized Configurations (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>work_mem</td>
<td></td>
<td>32768 KB</td>
</tr>
<tr>
<td>maintenance_work_mem</td>
<td></td>
<td>32768 KB</td>
</tr>
<tr>
<td>max_fsm_pages</td>
<td></td>
<td>200000 disk pages</td>
</tr>
<tr>
<td>checkpoint_segments</td>
<td></td>
<td>64 log file segments</td>
</tr>
<tr>
<td>checkpoint_timeout</td>
<td></td>
<td>600 seconds</td>
</tr>
<tr>
<td>Device Server</td>
<td>profilerMgr.receiver.maxParallelConns</td>
<td>Reduce from 3 to 1</td>
</tr>
</tbody>
</table>

See “Setting Preferences to Improve Profiler Performance” on page 212 for more information on recommended settings.

### High-End Configuration (9 to 20 IDP Profiling Devices)

Table 35 on page 211 describes recommendations for optimum performance when managing 9 to 20 profiling devices.

### Table 35: Performance Turning Recommendations for High-End Configurations

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Setup</td>
<td>GUI Server and Device Server (Profiler DB) running on the separate machines</td>
<td>N/A</td>
</tr>
<tr>
<td>Physical Memory Required</td>
<td></td>
<td>8 GB</td>
</tr>
<tr>
<td>CPU</td>
<td></td>
<td>4 Fast</td>
</tr>
<tr>
<td>Disk space reserved for Profiler.</td>
<td>*High-end SCSI drives preferred</td>
<td>24 GB</td>
</tr>
<tr>
<td>UI System Preferences</td>
<td>Purge profiler database if size exceeds</td>
<td>8000 MB</td>
</tr>
<tr>
<td>Max profiler database size after purging</td>
<td></td>
<td>6000 MB</td>
</tr>
<tr>
<td>PostgreSQL Settings</td>
<td>shared_buffers</td>
<td>262143 KB</td>
</tr>
<tr>
<td></td>
<td>work_mem</td>
<td>512000 KB</td>
</tr>
<tr>
<td></td>
<td>maintenance_work_mem</td>
<td>32768 KB</td>
</tr>
</tbody>
</table>
Table 35: Performance Turning Recommendations for High-End Configurations (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_fsm_pages</td>
<td></td>
<td>2000000 disk pages</td>
</tr>
<tr>
<td>checkpoint_segments</td>
<td></td>
<td>128 log file segments</td>
</tr>
<tr>
<td>checkpoint_timeout</td>
<td></td>
<td>3600 seconds</td>
</tr>
</tbody>
</table>

See “Setting Preferences to Improve Profiler Performance” on page 212 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 36 on page 212 describes settings that you can configure to improve performance from the UI.

Table 36: Profiler Settings in UI System Preferences

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB Max Size—Purge Profiler Database if size exceeds (in MB)</td>
<td>A background Auto Purge is triggered if the Profiler database size exceeds this limit.</td>
<td>3000 MB</td>
</tr>
<tr>
<td>DB Max Size After Purge</td>
<td>Auto Purge attempts to bring down the Profiler database size to less than this limit.</td>
<td>2200 MB</td>
</tr>
<tr>
<td>Profiler Query Timeout (in seconds)</td>
<td>The SQL query times out 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.</td>
<td>120 seconds</td>
</tr>
</tbody>
</table>
Table 36: Profiler Settings in UI System Preferences (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hour of day to perform database optimization (local time)</td>
<td>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.</td>
<td>7 GMT</td>
</tr>
</tbody>
</table>

PostgreSQL Server

You can also configure settings on the PostgreSQL server to improve the performance of the 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 37 on page 213 describes parameters in the `postgresql.conf` file that affect Profiler performance.

Table 37: PostgreSQL Server Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>shared_buffers</td>
<td>Sets the number of shared memory buffers (each 8 KB) used by the database server. Minimum is 2 X max_connections</td>
<td>1000 KB</td>
</tr>
<tr>
<td>work_mem</td>
<td>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.</td>
<td>16384 KB</td>
</tr>
<tr>
<td>maintenance_work_mem</td>
<td>Specifies the maximum amount of memory to be used in maintenance operations, such as VACUUM. The value is specified in kilobytes.</td>
<td>8192 KB</td>
</tr>
<tr>
<td>max_fsm_pages</td>
<td>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.</td>
<td>20000</td>
</tr>
<tr>
<td>checkpoint_segments</td>
<td>Maximum distance between automatic checkpoints maintained by postgresql, in log file segments.</td>
<td>64</td>
</tr>
<tr>
<td>checkpoint_timeout</td>
<td>Maximum time between automatic checkpoints, in seconds.</td>
<td>600 seconds</td>
</tr>
</tbody>
</table>
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:

$NSROOT/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_shmmin=1  
set shmsys:shminfo_shmmni=256  
set semsys:seminfo_numsem=256  
set semsys:seminfo_numshmem=512  
set semsys:seminfo_nummsg=512  
set semsys:seminfo_cache=32
```

On Linux systems, add/update the following line in `/etc/sysctl.conf`:

```
kernal.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 Profiler DB. Table 38 on page 214 describes parameters in the Device Server configuration file (`devSvr.cfg`) that affect performance.

**Table 38: Device Server Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>profilerMgr.printLevel</td>
<td>For debugging, info is most useful, but will potentially generate lots of logs.</td>
<td>Notice</td>
</tr>
<tr>
<td>profilerMgr.receiver.pktIntTimeoutInSec</td>
<td>A profiler session times out of time exceeds this configured value.</td>
<td>300 seconds</td>
</tr>
</tbody>
</table>
Table 38: Device Server Settings (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>profilerMgr.receiver.saveFailedData</td>
<td>Profiler Data of a profiler session is stored temporarily in the folder $NSROOT/DevSvr/var/profiler_data/domainId. If a session completes successfully this folder is cleaned up. Otherwise, the folder is cleaned up unless this setting is 'YES'.</td>
<td>NO</td>
</tr>
<tr>
<td>profilerMgr.receiver.maxParallelConns</td>
<td>Specifies maximum number of concurrent profiler sessions.</td>
<td>3</td>
</tr>
<tr>
<td>profilerMgr.receiver.minPollTimeInSec</td>
<td>Two consecutive profiler sessions for the same device is spaced apart by at least this interval.</td>
<td>300 seconds</td>
</tr>
<tr>
<td>profilerMgr.receiver.vacuumCostDelay</td>
<td>The length of time, in milliseconds, that the vacuum process will sleep when the vacuumCostLimit has been exceeded.</td>
<td>0 msec</td>
</tr>
<tr>
<td>profilerMgr.receiver.vacuumCostLimit</td>
<td>The accumulated cost that will cause the vacuuming process to sleep.</td>
<td>200 msec</td>
</tr>
<tr>
<td>profilerMgr.receiver.minVacuumInterval</td>
<td>Minimum time interval between two consecutive vacuums.</td>
<td>300 seconds</td>
</tr>
<tr>
<td>profilerMgr.receiver.performVacuumFull</td>
<td>If this setting is 'YES', VACUUM FULL is performed during optimization otherwise skipped.</td>
<td>NO</td>
</tr>
<tr>
<td>profilerMgr.receiver.optimizationWindow</td>
<td>This specifies the time window in hours from the 'hour to perform optimization' setting of GUI &gt;System Preferences &gt;Profiler Settings. Optimization would be triggered only during this window.</td>
<td>3 hours</td>
</tr>
<tr>
<td>profilerMgr.profilerQuerier.profilerQueryTimeoutInterval</td>
<td>A GUI query session is timed out if there is no activity for this interval.</td>
<td>600 seconds</td>
</tr>
</tbody>
</table>

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
```
PART 3

Index

- Index on page 219
Index

A
adding, Device Server............................................................62

B
bulk cli timeout.......................................................................187

C
Central Manager, upgrading.....................................157, 162
configuration options
  database backup.......................................................................10
  installing management system on same server (typical)...............8
  installing management system on separate servers (extended).....8
  Statistical Report Server...................................................10
configuring
  HA Cluster..........................................................................107
  high availability......................................................................180
  management system IP addresses.................................175
CPU
  requirements on management system, same server.....................5
  requirements on management system, separate servers.............6
customer support..................................................................xx
  contacting JTAC...............................................................xx

D
data directory
  for Device Server, described...............22, 50, 80, 132
  for GUI Server, described...............23, 51, 80, 132
data migration.......................................................................165
database
  backup options.....................................................................10
  replicating.........................................................................181
  restoring..........................................................................182
defining system parameters..................................................22, 50, 79, 132
Demo Mode..............................................................................47
Device Server
  adding..................................................................................62
  installing.............................................................................63
  starting.............................................................................173
Device Server ID
  described..............................................................................52, 83, 134
disk storage
  requirements on management system, same server...................5
  requirements on management system, separate servers............6
downgrading...........................................................................188
E
establishing
  SSH trust relationship......................................................85
extended configuration option..................................................8
G
GUI Server
  installing..............................................................................53
  starting.............................................................................173
  stopping.............................................................................173
H
HA cluster
  configuring.........................................................................107
HA Server
  starting.............................................................................172
  stopping.............................................................................173
heartbeat communications
  described..........................................................................74
heartbeat links
  described..........................................................................81
high availability
  configuring manually.......................................................180
  installing.............................................................................72
  overview.............................................................................9
I
installation
CD.................................................................4
log file for management system........35, 58, 93
log file for UI..................................................44
package................................................................4
installing
configuration options.........................7
management system on same server......21
management system on separate
    servers..........................................................49, 78
management system with high availability -
    separate servers.............................................110
prerequisite steps...........................................24
TFTP server on Linux..............................186
TFTP server on Solaris..............................186
UI........................................................................40
Installing
Device Server.............................................63
GUI Server..................................................53
L
license keys
    described......................................................13
Linux, migration to NSMXpress............167
locales, Solaris...........................................28, 140
log file
    management system install.....................35
    UI installation.............................................44
logging in to the UI..............................45
logs
    restoring....................................................179
M
management
    installing on separate servers...............49
management IP address
    for GUI Server, described.......................23, 51, 80, 133
management system
    commands..................................................171
    installing on same server........................21
    installing on separate servers................78
    restarting..................................................172
    starting.....................................................172
    status.........................................................172
    stopping....................................................172
    uninstalling..............................................188
    upgrading................................................131
    upgrading Central Manager.....................157, 162
    upgrading NSMXpress.................................155, 160
memory requirements
    for UI..........................................................7
    management system on same server...........5
    management system on separate servers.....6
migration to NSMXpress........................165
minimum system requirements
    for UI..........................................................7
    management system....................................5
N
network connection
    requirements for UI.................................7
    requirements on management system, same
        server....................................................5
    requirements on management system,
        separate servers.....................................6
NSM inbound ports...............................196
NSM outbound ports..............................197
NSMXpress
    migration from Linux.............................167
    migration from Solaris.............................165
    upgrading................................................155, 160
    user privileges for....................................169
O
operating system
    requirements for management system........5
    requirements for UI.....................................7
overview
    high availability.........................................9
P
Password for GUI Server connection
    described..................................................52, 83, 134
prerequisites before installing..................24
prerequisites before upgrading..................137
process
    for installing management system............3
    for installing UI.........................................4
R
replicating
    database....................................................181
restarting management system................172
restoring
    database....................................................182
    logs and configuration data......................179
rsync
   using with database backup.................................10
running
   UI...........................................................................45
   UI, in Demo Mode.......................................................47
S
Solaris
   migration to NSMXpress........................................165
   preparing for NSM....................................................28, 140
   required locales.....................................................28, 140
SSH trust relationship
   establishing................................................................85
starting
   Device Server............................................................173
   GUI Server................................................................173
   HA Server..................................................................172
   management system manually.................................172
Statistical Report Server
   installing with NSM...................................................10
stopping
   GUI Server...............................................................173
   HA Server..................................................................173
   management system manually.................................172
superuser
   password, described.............................................23, 51, 80, 133
support, technical See technical support
swap space
   requirements on management system, same
      server..................................................................5
   requirements on management system,
      separate servers....................................................6
system parameters..................................................................22, 50, 79, 132
system update utility
   described......................................................................5
   running.......................................................................25, 138
T
technical support
   contacting JTAC..........................................................xx
TFTP server
   installing on Linux......................................................186
   installing on Solaris......................................................186
timeout
   bulk cli modification................................................187
   typical configuration option......................................8
U
UI
   installation process.....................................................4
   installing......................................................................40
   running......................................................................45
   uninstalling................................................................190
   upgrading.....................................................................149
uninstalling
   UI................................................................................190
upgrading
   management system...................................................131
   management system on separate servers.................150
   prerequisite steps....................................................137
   UI..............................................................................149
Upgrading
   Central Manager......................................................157, 162
   NSMXpress.................................................................160
   NSMXpress, ...............................................................155
User privileges, setting for NSMXpress......................169
V
validating
   database recovery......................................................182
   management system installation..........................45
   management system status.................................39, 69, 94, 149
   management system upgrade...............................150
   viewing management system commands..................171