Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

Copyright © 2016 Novell, Inc. All Rights Reserved.
# Contents

About This Guide .......................................................... 7

1 Overview of Novell Remote Manager for Linux ........................................... 9
   1.1 Benefits of Using Novell Remote Manager ........................................... 9
   1.2 Other Management Utilities .......................................................... 10
   1.3 What's Next ................................................................................. 10

2 What's New or Changed in Novell Remote Manager ...................................... 13
   2.1 What's New (OES 2015 SP1) ......................................................... 13
   2.2 What's New (OES 2015) ................................................................ 13

3 Migrating Novell Remote Manager from NetWare to OES 2015 SP1 .................. 15
   3.1 Coexistence ................................................................................. 15
      3.1.1 Compatibility ....................................................................... 15
      3.1.2 Coexistence Issues .............................................................. 15
   3.2 Migration .................................................................................... 15

4 Managing a Virtualized Linux Server with Novell Remote Manager ................. 17

5 Installing Novell Remote Manager for Linux ................................................. 19
   5.1 Installing Novell Remote Manager During the Initial Server Installation ... 19
   5.2 Installing Novell Remote Manager After the Initial Server Installation .... 19

6 Accessing Novell Remote Manager for Linux ................................................. 21
   6.1 System Requirements .................................................................... 21
   6.2 Accessing Novell Remote Manager ............................................... 22
   6.3 Starting or Stopping HTTPSTKD ............................................... 24
   6.4 Understanding the Layout of Novell Remote Manager .................... 24
      6.4.1 Header Frame ....................................................................... 27
      6.4.2 Overall Health Indicator ..................................................... 27
      6.4.3 Navigation Frame .................................................................. 28
      6.4.4 Program Plug-Ins in the Navigation Frame ......................... 29
      6.4.5 Main Content Frame .......................................................... 29
      6.4.6 Online Help ....................................................................... 29
   6.5 Accessing Configuration Options .................................................. 29
   6.6 Accessing Online Help .................................................................. 30
   6.7 Accessing Novell Web Pages ......................................................... 30

7 Changing the HTTPSTKD Configuration ....................................................... 31
   7.1 Accessing and Editing the HTTPSTKD Configuration File ................. 33
   7.2 Accessing and Editing the HTTPSTKD PAM Configuration File ........ 34
   7.3 Restarting the HTTPSTKD Daemon .............................................. 35
   7.4 Viewing the HTTP Logs ............................................................... 35
# Diagnosing Problems Using Ganglia and Nagios (OES 2015 SP1)

8.1 Monitoring Server Health .............................................. 39
  8.1.1 Viewing the Overall Server Health Status .................... 40
  8.1.2 Setting the Health Status Refresh Rate ...................... 40
8.2 Configuring Ganglia ................................................ 41
  8.2.1 Ganglia Requirements ........................................... 41
  8.2.2 Configuring Ganglia gmond in Multicast Mode or Unicast Mode 42
8.3 Stopping and Starting Ganglia gmond and gmetad ................. 44
8.4 Monitoring Server Health with Ganglia ........................ 44
8.5 Configuring Nagios ................................................ 47
  8.5.1 Configuring Nagios Authenticated Users and Contacts ...... 47
  8.5.2 Configuring Nagios Monitoring ................................ 51
  8.5.3 Accessing the Nagios Website ................................ 53
  8.5.4 Using Nagios Plug-Ins ......................................... 53
  8.5.5 Using Object Configuration Files ............................ 54
  8.5.6 Additional Information ....................................... 54
8.6 Monitoring Service Health with Nagios ......................... 54
8.7 Restarting Nagios .................................................. 55
8.8 Managing Nagios Users ............................................. 55
  8.8.1 Creating or Re-Creating a Nagios User ....................... 55
  8.8.2 Setting Passwords for Nagios Users ........................ 56
  8.8.3 Deleting a Nagios User ....................................... 56
  8.8.4 Configuring Nagios Contacts and Notification Methods for Them 57
  8.8.5 Configuring Nagios CGI Authorization for Contacts .......... 57
8.9 Modifying the Nagios Notification Methods for Contacts ....... 58
8.10 Configuring Nagios Logging ....................................... 58
8.11 Viewing the PIDs or Monitoring the Health of Processes ...... 60
8.12 Monitoring or Killing an Individual Process .................... 61
8.13 Troubleshooting a Suspect or Bad Health Status .......... 62

# Viewing File Systems

9.1 Viewing Mounted Devices and Performing Actions on Them .... 64
9.2 Browsing File Systems and Performing Actions on Them .......... 65
  9.2.1 Viewing or Changing File or Directory Attributes .......... 67
  9.2.2 Viewing Details about Directories and Performing Actions on Them 67
  9.2.3 Uploading a File to the Server ................................ 68
  9.2.4 Downloading a File from the Server to a Local Workstation 68
  9.2.5 Searching for Text in Files .................................. 69
  9.2.6 Viewing the Details of a File and Performing Specific Actions 69
  9.2.7 Viewing Individual Files .................................... 70
9.3 Viewing Partition Information .................................... 70

# Managing Linux

10.1 Accessing VNC Consoles .......................................... 71
10.2 Viewing Kernel Modules ......................................... 73
10.3 Shutting Down and Restarting the Host .......................... 74
10.4 Managing Packages ............................................. 75
10.5 Managing Processes ............................................... 76
10.6 Scheduling cron Jobs to Run on the Server ...................... 78
11 Managing Hardware
11.1 Viewing Processors ................................................. 81
11.2 Viewing Interrupt Information ................................. 82
11.3 Viewing I/O Memory Information ............................. 83
11.4 Viewing I/O Port Information ................................. 84
11.5 Viewing SMBIOS Information .................................. 85

12 Using Group Operations
12.1 Building and Configuring a Monitoring Group ............... 88
12.2 Saving a Group .................................................... 92
12.2.1 Saving the Group to the Local Server .................... 92
12.2.2 Saving the Group and Associating It with an eDirectory Object ............................................ 92
12.3 Accessing an Existing Group ................................... 93
12.4 Changing an Existing Group .................................... 93
12.5 Deleting an Existing Group ..................................... 94
12.6 Generating and Viewing Server Reports ....................... 94
12.6.1 Compare Server Up Time Report ......................... 94
12.7 Viewing Monitored Items ....................................... 95
12.8 Viewing Group Monitoring Types ............................. 95
12.9 Defining or Editing Group Monitoring Types ................ 96
12.10 Discovering Items on the Network to Monitor ............. 97

13 Managing NCP Services
13.1 Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux .............................. 100
13.1.1 NCP Volumes (NCP Shares) ............................... 101
13.1.2 NCP Server Parameters .................................... 102
13.1.3 NCP Server Connections .................................. 102
13.1.4 NCP Trustee Reports ...................................... 103
13.1.5 NCP Logs and Audit Logs ................................. 103
13.1.6 NCP Server Statistics ..................................... 104
13.1.7 NCP Server Diagnostics ................................... 104
13.1.8 Dynamic Storage Technology ............................. 105
13.2 Browsing NSS Volumes and Performing Actions on Them ................................................................. 106
13.2.1 Viewing Information about an NSS Volume .............. 106
13.2.2 Viewing the Linux POSIX Details of an NSS Directory and Performing Specific Actions on It ......................... 108
13.2.3 Viewing the Linux POSIX Details of a File and Performing Specific Actions on It ................................ 109
13.2.4 Browsing an NSS Volume and Setting Rights and File System Attributes on Directories and Files ........................................... 110
13.2.5 Salvaging and Purging Deleted Files on an NSS Volume ...................................................... 114
13.2.6 Purging a Deleted NSS Volume ............................ 114
13.2.7 Viewing Open File Information for an NSS Volume .................. 115
13.3 Generating Inventories for Directories or NCP Volumes ................................................................. 115
13.3.1 Generating a File Inventory Report ...................... 116
13.3.2 Generating an NCP Volume Inventory Report ........... 118
13.3.3 Viewing a Saved NCP Inventory Report ................ 120
13.3.4 Emailing a Saved NCP Inventory Report (OES 11 SP1) ...................................................... 120
13.4 Generating a Custom Inventory Report from a File Inventory Report ........................................... 121
13.5 Performing Actions on Files from Custom Reports ......... 122
13.5.1 Moving Selected Files ....................................... 122
13.5.2 Copying Selected Files ...................................... 122
13.5.3 Deleting Selected Files ...................................... 123
13.5.4 Opening or Downloading a File ............................ 123
13.5.5 Managing Individual Files .................................. 123
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.6</td>
<td>Generating and Viewing NCP Trustee Reports for NSS Volumes</td>
<td>123</td>
</tr>
<tr>
<td>13.6.1</td>
<td>Generating an NCP Trustee Report</td>
<td>124</td>
</tr>
<tr>
<td>13.6.2</td>
<td>Viewing a Saved NCP Trustee Report</td>
<td>124</td>
</tr>
<tr>
<td>13.6.3</td>
<td>Emailing a Saved NCP Trustee Report (OES 11 SP1)</td>
<td>124</td>
</tr>
<tr>
<td>14</td>
<td>Managing Dynamic Storage Technology Options</td>
<td>127</td>
</tr>
<tr>
<td>15</td>
<td>Managing CIFS Services</td>
<td>131</td>
</tr>
<tr>
<td>15.1</td>
<td>Managing CIFS Connections</td>
<td>131</td>
</tr>
<tr>
<td>15.2</td>
<td>Viewing Log Information</td>
<td>132</td>
</tr>
<tr>
<td>15.3</td>
<td>Managing Open Files</td>
<td>132</td>
</tr>
<tr>
<td>16</td>
<td>Managing AFP Services</td>
<td>135</td>
</tr>
<tr>
<td>16.1</td>
<td>Managing AFP Connections</td>
<td>136</td>
</tr>
<tr>
<td>16.2</td>
<td>Viewing Log Information</td>
<td>136</td>
</tr>
<tr>
<td>16.3</td>
<td>Managing Open Files</td>
<td>137</td>
</tr>
<tr>
<td>17</td>
<td>Tasks Quick Reference</td>
<td>139</td>
</tr>
<tr>
<td>18</td>
<td>Troubleshooting Novell Remote Manager</td>
<td>143</td>
</tr>
<tr>
<td>18.1</td>
<td>Daemon httpstkd Is Unable to Start</td>
<td>143</td>
</tr>
<tr>
<td>18.2</td>
<td>Error while loading shared libraries: libldap.so.0</td>
<td>143</td>
</tr>
<tr>
<td>18.3</td>
<td>Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 2015 SP1</td>
<td>144</td>
</tr>
<tr>
<td>18.4</td>
<td>Ganglia Statistical Graphics Are Not Displayed in the Web Browser</td>
<td>145</td>
</tr>
<tr>
<td>18.4.1</td>
<td>Firefox</td>
<td>145</td>
</tr>
<tr>
<td>18.4.2</td>
<td>Internet Explorer</td>
<td>146</td>
</tr>
<tr>
<td>18.4.3</td>
<td>Chrome</td>
<td>146</td>
</tr>
<tr>
<td>19</td>
<td>Security Considerations</td>
<td>147</td>
</tr>
<tr>
<td>19.1</td>
<td>Security Features</td>
<td>147</td>
</tr>
<tr>
<td>19.2</td>
<td>Security Characteristics</td>
<td>149</td>
</tr>
<tr>
<td>19.3</td>
<td>Security Configuration</td>
<td>149</td>
</tr>
<tr>
<td>19.4</td>
<td>Nagios Security Configuration</td>
<td>151</td>
</tr>
<tr>
<td>A</td>
<td>HTTPSTKD Configuration File Options</td>
<td>153</td>
</tr>
<tr>
<td>A.1</td>
<td>Address and Port Commands</td>
<td>153</td>
</tr>
<tr>
<td>A.2</td>
<td>Disable Auto LUM Command</td>
<td>154</td>
</tr>
<tr>
<td>A.3</td>
<td>Email Notification Commands (OES 11 SP1 and Earlier)</td>
<td>156</td>
</tr>
<tr>
<td>A.4</td>
<td>Filtering Commands</td>
<td>157</td>
</tr>
<tr>
<td>A.5</td>
<td>HttpOnly Command</td>
<td>158</td>
</tr>
<tr>
<td>A.6</td>
<td>InventoryResolveNonLumOwnerName Command</td>
<td>159</td>
</tr>
<tr>
<td>A.7</td>
<td>Language Commands</td>
<td>159</td>
</tr>
<tr>
<td>A.8</td>
<td>Load Command</td>
<td>161</td>
</tr>
<tr>
<td>A.9</td>
<td>SSL Key Cipher Strength Command</td>
<td>162</td>
</tr>
<tr>
<td>A.10</td>
<td>Supervisor Only Command</td>
<td>162</td>
</tr>
<tr>
<td>B</td>
<td>Novell Remote Manager Packages</td>
<td>165</td>
</tr>
</tbody>
</table>
About This Guide

This guide describes how to access and use Novell Remote Manager on a host that is running Open Enterprise Server (OES) 2015 SP1 on the SUSE Linux Enterprise Server (SLES) 11 Service Pack 4 (SP4) operating system. This guide includes the following information:

- Chapter 1, “Overview of Novell Remote Manager for Linux,” on page 9
- Chapter 2, “What’s New or Changed in Novell Remote Manager,” on page 13
- Chapter 3, “Migrating Novell Remote Manager from NetWare to OES 2015 SP1,” on page 15
- Chapter 4, “Managing a Virtualized Linux Server with Novell Remote Manager,” on page 17
- Chapter 5, “Installing Novell Remote Manager for Linux,” on page 19
- Chapter 6, “Accessing Novell Remote Manager for Linux,” on page 21
- Chapter 7, “Changing the HTTPSTKD Configuration,” on page 31
- Chapter 8, “Diagnosing Problems Using Ganglia and Nagios (OES 2015 SP1),” on page 39
- Chapter 9, “Viewing File Systems,” on page 63
- Chapter 10, “Managing Linux,” on page 71
- Chapter 11, “Managing Hardware,” on page 81
- Chapter 12, “Using Group Operations,” on page 87
- Chapter 13, “Managing NCP Services,” on page 99
- Chapter 14, “Managing Dynamic Storage Technology Options,” on page 127
- Chapter 15, “Managing CIFS Services,” on page 131
- Chapter 16, “Managing AFP Services,” on page 135
- Chapter 17, “Tasks Quick Reference,” on page 139
- Chapter 18, “Troubleshooting Novell Remote Manager,” on page 143
- Chapter 19, “Security Considerations,” on page 147
- Appendix A, “HTTPSTKD Configuration File Options,” on page 153
- Appendix B, “Novell Remote Manager Packages,” on page 165

Audience

This guide is intended for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to Novell Documentation Feedback (http://www.novell.com/documentation/feedback.html) and enter your comments there.
Documentation Updates

For the most recent version of the *Novell Remote Manager Administration Guide*, visit the OES 2015 documentation website (http://www.novell.com/documentation/oes2015/mgmt_remotemgr_lx/data/front.html).

Additional Documentation

For information about other OES 2015 services and file systems, see the OES 2015 documentation website (http://www.novell.com/documentation/oes2015/).
Overview of Novell Remote Manager for Linux

Novell Remote Manager for Linux is a browser-based utility that you can use to manage one or more Linux servers from a remote location.

You can use Novell Remote Manager to monitor your server’s health, change the configuration of your server, or perform diagnostic and debugging tasks.

The advantages of using Novell Remote Manager for server management are that:

- It does not require a special client.
- It provides a graphical interface that makes interpreting diagnostic information much more comprehensive and easier to manage.
- It provides added functionality that is not available in the other management utilities.

This section explains the following:

- Section 1.1, “Benefits of Using Novell Remote Manager,” on page 9
- Section 1.2, “Other Management Utilities,” on page 10
- Section 1.3, “What’s Next,” on page 10

1.1 Benefits of Using Novell Remote Manager

Organizations usually don’t have a technician physically located at the server when it needs attention. Servers are frequently placed in remote or distributed locations and, in the case of service providers, at many different companies. The ability to centrally monitor, diagnose, and repair (or preventively avoid) server problems is a significant advantage. It is also a major benefit to be able to provide technical service from any location—any point in the world—across the Internet.

Novell Remote Manager provides IT staff and service providers the ability to monitor and control a complete selection of server controls and functions through a standard web browser.

The management power and flexibility now available simplifies network administration and allows fewer staff to effectively manage more resources. Novell Remote Manager lets you do the following:

- Securely access and manage a Linux server from any location. With proper login credentials and Internet access, administrators can control servers from any location.
- Group servers for collective management, allowing you to manage multiple servers through the same interface and application.
- Quickly locate and assess problems. An intuitive graphical user interface provides a control dashboard with indicators for server health and status.
- Manage servers comprehensively. Novell Remote Manager provides control for viewing or managing Linux servers, directories, processes, and hardware.
While using Novell Remote Manager, you can perform the following major tasks:

- Monitor and manage your server’s health
  - Monitor the health status of one or more servers
  - Build a group of servers and items to be monitored together
  - Access server and configuration logs
- Configure your server
  - View information about all hardware adapters, hardware resources, and processor data
  - Upload and replace files
  - Monitor memory resources
  - Access files
  - Shut down or reset a server
- Troubleshoot server problems
  - Find high memory users
  - Monitor server processes

### 1.2 Other Management Utilities

Novell Remote Manager does not replace other management utilities that are available in OES. For an understanding of which utilities are best for the task you need to perform, see “OES Utilities and Tools” in the OES 2015 SP1: Planning and Implementation Guide.

### 1.3 What's Next

Now that you have learned some of the benefits of using Novell Remote Manager, use the information in Table 1-1 and Table 1-2 to help you access and use it.

**Table 1-1 Information about Novell Remote Manager**

<table>
<thead>
<tr>
<th>For Information About</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing and understanding the layout of Novell Remote Manager</td>
<td>Chapter 6, “Accessing Novell Remote Manager for Linux,” on page 21</td>
</tr>
<tr>
<td>Determining whether Novell Remote Manager for Linux is compatible</td>
<td>Chapter 3, “Migrating Novell Remote Manager from NetWare to OES 2015 SP1,” on page 15</td>
</tr>
<tr>
<td>and how it fits in your current network</td>
<td></td>
</tr>
<tr>
<td>Managing a virtualized OES server with Novell Remote Manager</td>
<td>Chapter 4, “Managing a Virtualized Linux Server with Novell Remote Manager,” on page 17</td>
</tr>
<tr>
<td>Installing Novell Remote Manager for Linux</td>
<td>Chapter 5, “Installing Novell Remote Manager for Linux,” on page 19</td>
</tr>
<tr>
<td>Changing the configuration of Novell Remote Manager</td>
<td>Chapter 7, “Changing the HTTPSTKD Configuration,” on page 31</td>
</tr>
</tbody>
</table>
### Table 1-2 Information about Plug-Ins to Novell Remote Manager

<table>
<thead>
<tr>
<th>For Information About</th>
<th>See</th>
</tr>
</thead>
</table>
| Using Novell Remote Manager to monitor and manage your OES servers | - Chapter 8, “Diagnosing Problems Using Ganglia and Nagios (OES 2015 SP1),” on page 39  
|                                                | - Chapter 9, “Viewing File Systems,” on page 63                      |
|                                                | - Chapter 10, “Managing Linux,” on page 71                          |
|                                                | - Chapter 11, “Managing Hardware,” on page 81                        |
|                                                | - Chapter 12, “Using Group Operations,” on page 87                   |
| Things to consider for setting up your system in a secure environment | Chapter 19, “Security Considerations,” on page 147                   |

### Things to consider for setting up your system in a secure environment.
What’s New or Changed in Novell Remote Manager

This section describes the changes made to Novell Remote Manager since the Open Enterprise Server (OES) 2015 release.

- Section 2.1, “What’s New (OES 2015 SP1),” on page 13
- Section 2.2, “What’s New (OES 2015),” on page 13

2.1 What’s New (OES 2015 SP1)

NRM in OES 2015 SP1 has been modified for bug fixes. There are no new features or enhancements in OES 2015 SP1.

2.2 What’s New (OES 2015)

In addition to bug fixes, OES 2015 provides the following enhancements and changes for NRM:

- **Support for NSS 64-Bit Pools and Volumes** Novell Remote Manager has been modified to support NSS 64-bit pools and volumes.
  
  The *OES 2015: Novell Remote Manager Administration Guide* has been modified throughout to accommodate the new 64-bit pools and volumes.

- **Support for Active Directory Users** You can now manage CIFS connections for AD users and view information for files they access.
  
  For more information, see Managing CIFS Connections in the *OES 2015: Novell Remote Manager Administration Guide*. 
3 Migrating Novell Remote Manager from NetWare to OES 2015 SP1

Novell Remote Manager for Open Enterprise Server (OES) 2015 SP1 runs on servers with OES 2015 SP1 services installed. This section contains information about the following:

- Section 3.1, “Coexistence,” on page 15
- Section 3.2, “Migration,” on page 15

3.1 Coexistence

- Section 3.1.1, “Compatibility,” on page 15
- Section 3.1.2, “Coexistence Issues,” on page 15

This section provides information regarding the compatibility and coexistence of Novell Remote Manager for OES with existing networks containing NetWare or OES platforms.

3.1.1 Compatibility

When you create a group, you can get server health status from a NetWare server running NetWare 6.0 or later or from an OES Linux server running OES 1 or later.

3.1.2 Coexistence Issues

Monitoring on Linux servers that are not running the owcimond module can report only an Up/Down status.

3.2 Migration

There is no need to migrate Novell Remote Manager from NetWare to Novell Remote Manager for Linux. Novell Remote Manager is selected for installation when any pattern from Open Enterprise Server is installed.

You can combine server groups for monitoring NetWare and OES servers. You can save the group file locally or to an eDirectory object. See “Saving a Group” on page 92 and “Accessing an Existing Group” on page 93.

Configuring Novell Remote Manager is somewhat different on an OES server than a NetWare server. See “Changing the HTTPSTKD Configuration” on page 31.

Some tasks that are available in Novell Remote Manager for NetWare are not available on Novell Remote Manager for Linux, such as IP Address Management. You have the functionality to monitor the server health for individual servers or groups of servers, the ability to load and unload programs, and access console screens.
The following features are available for Novell Remote Manager for Linux that are not available for NetWare:

- Dynamic Storage Technology. For information, see *OES 2015 SP1: Dynamic Storage Technology Administration Guide*.
- NCP (NetWare Control Protocol) server and NCP volumes (shares) on Linux POSIX file systems. For information, see *OES 2015 SP1: NCP Server for Linux Administration Guide*. 
Managing a Virtualized Linux Server with Novell Remote Manager

Using Novell Remote Manager for Linux to access and manage a virtualized Open Enterprise Server (OES) 11 or later server is the same in every way as accessing and managing a physical OES 11 or later server. It requires no special configuration or other changes.


For information about setting up virtualized OES, see “Installing, Upgrading, or Updating OES on a VM” in the OES 2015 SP1: Installation Guide.

To get started with third-party virtualization platforms, such as Hyper-V from Microsoft and the different VMware product offerings, refer to the documentation for the product you are using.
Novell Remote Manager is installed as a Open Enterprise Server (OES) 2015 SP1 service pattern in the YaST Install. This section contains the following information:

- Section 5.1, “Installing Novell Remote Manager During the Initial Server Installation,” on page 19
- Section 5.2, “Installing Novell Remote Manager After the Initial Server Installation,” on page 19

### 5.1 Installing Novell Remote Manager During the Initial Server Installation

To install Novell Remote Manager during the OES 2015 SP1 installation or while adding OES 2015 SP1 on an existing server, select the Novell Remote Manager (NRM) pattern to install Novell Remote Manager.

It does not require any additional configuration during the installation and does not display on the Installation Settings page. For information about changing the configuration after the installation is complete, see Chapter 7, “Changing the HTTPSTKD Configuration,” on page 31.

For a list of RPMs that it installs, see Appendix B, “Novell Remote Manager Packages,” on page 165.

### 5.2 Installing Novell Remote Manager After the Initial Server Installation

If you did not install Novell Remote Manager when you first installed OES 2015 SP1, do the following to install and configure Novell Remote Manager:

1. Open YaST.
2. Click Open Enterprise Server > OES Install and Configuration.
3. Select the Novell Remote Manager (NRM) pattern.
   
   Selecting this pattern automatically selects the Novell Linux User Management (LUM) and Novell Backup/Storage Management Services (SMS) patterns.

4. (Conditional) If you want only the Novell Remote Manager pattern installed, deselect the Novell Linux User Management (LUM) and Novell Backup/Storage Management Services (SMS) patterns.

   If you have only Novell Remote Manager installed, then you can log in to Novell Remote Manager only as user root or a local Linux user.

   If you log in as a local Linux user, you can see only the information that the user you log in as has rights to view.

5. Click Accept.

6. If necessary, complete any required information for other services selected on the Micro Focus Open Enterprise Server Configuration summary page. When all the settings on the Micro Focus Open Enterprise Server Configuration summary page are set as desired, click Next.
The necessary files are installed and configuration of the services are completed.

No additional configuration during the installation for Novell Remote Manager is required. For information about changing the configuration after the installation is complete, see Chapter 7, “Changing the HTTPSTKD Configuration,” on page 31.

For a list of RPMs that it installs, see Appendix B, “Novell Remote Manager Packages,” on page 165.
6 Accessing Novell Remote Manager for Linux

This section includes information about the following:

- Section 6.1, “System Requirements,” on page 21
- Section 6.2, “Accessing Novell Remote Manager,” on page 22
- Section 6.3, “Starting or Stopping HTTPSTKD,” on page 24
- Section 6.4, “Understanding the Layout of Novell Remote Manager,” on page 24
- Section 6.5, “Accessing Configuration Options,” on page 29
- Section 6.6, “Accessing Online Help,” on page 30
- Section 6.7, “Accessing Novell Web Pages,” on page 30

6.1 System Requirements

☐ Supported web browsers:
  - Mozilla Firefox 12 or later
  - Microsoft Internet Explorer (IE) 8 and 9. IE 10 and 11 is supported for Windows 7 and 8 clients in the desktop view only.
  - Apple Safari 5 and Safari 6.0 (for Mac OS X Mountain Lion (version 10.8) clients only)
  - Google Chrome 21 or later
  - KDE Konqueror 4 or later, with limited functionality

☐ Certificate handling requires SSL 2.0 or later or TLS 1.0 or later to be enabled in your web browser. Otherwise, the browser displays an error indicating that the page cannot be displayed. We recommend the higher security options of SSL 3.0 or the latest TLS if it is available.

☐ The HTTPSTKD package must be loaded and running on the server.

For information about starting or restarting the httpstkd daemon, see Section 6.3, “Starting or Stopping HTTPSTKD,” on page 24.

This package is selected for installation by the Novell Remote Manager pattern. The Novell Remote Manager (NRM) pattern is selected for installation when you install any of the OES Services patterns on Linux unless you deselect it.

For information about installing Novell Remote Manager, see Chapter 5, “Installing Novell Remote Manager for Linux,” on page 19.

For package details, see “Novell Remote Manager Packages” on page 165.
6.2 Accessing Novell Remote Manager

You typically log in as the Linux root user to manage all functions in Novell Remote Manager. The root user can access Novell Remote Manager even when eDirectory is not available.

Some functions support access by administrator users who are eDirectory users and who are also enabled for Linux with Linux User Management (LUM-enabled). If LUM is enabled in your tree and it is installed and configured on the server, you can log in to Novell Remote Manager using your eDirectory credentials. For instructions on enabling Linux, see “Setting Up Linux Computers to Use eDirectory Authentication” in the OES 2015 SP1: Linux User Management Administration Guide.

If you log in as a local Linux user or as a non-Admin LUM-enabled eDirectory user, you can see only the information that the user has rights to view. Typically, access is restricted to a view of the Linux file systems where the user has file system access rights.

There are two specific things to remember when logging in to Novell Remote Manager as a LUM-enabled eDirectory user:

- If eDirectory and LUM are installed on the local server, the eDirectory user Admin can log in to Novell Remote Manager using its fully distinguished name (admin.context) because this user is enabled for Linux User Management by default in this case.

In order for a user to log in to Novell Remote Manager as user Admin or equivalent, you must configure either of the following permissions for the Admin user:

- The Admin user must be associated to the group that has the Supervisor right for the Entry Rights property for the UNIX Workstation object.
- The Admin user must have the Supervisor right for the Entry Rights to the NCP object that represents the Linux server in the eDirectory tree.

**IMPORTANT:** With either of these permissions, the eDirectory user is granted limited root user privileges when logged in to the server. The user can modify only the configuration files necessary for configuring NRM or any other files that NRM has been assigned rights to allow modifying.

- In order for non-Admin users to log in using eDirectory credentials, they must be users enabled for Linux User Management.

Users who are enabled for Linux User Management have a Linux Profile tab on their Modify User page in iManager. They also have an eDirectory object that is associated with the UNIX Workstation object that represents the Linux server.

You can use iManager or the LUM command line utility namuseradd to enable users for Linux User Management. For instructions, see “Overview” in the OES 2015 SP1: Linux User Management Administration Guide.

The Admin user has limited file system rights equivalent to root. The user can modify only the configuration files necessary for configuring NRM or any other files that NRM has been assigned rights to allow modifying. For a list of these files, see Section 19.1, “Security Features,” on page 147. The user Admin or equivalent user has access according to the Linux and LUM file rights to all other files.
To access to Novell Remote Manager:

1. Open a web browser.
2. Point the browser to the URL of the server you want to manage by entering the following in the Address (URL) field:

   http://server_ip_address:8008

   or

   https://server_ip_address:8009

   If you specify HTTP and port 8008, you are automatically re-directed to use secure HTTP (HTTPS) and port 8009.

   For example, either of the following URLs take you to a secure SSL login page for Novell Remote Manager on the specified server:

   http://172.16.123.11:8008

   https://172.16.123.11:8009

3. Accept the SSL certificate.

   Certificate handling requires SSL 2.0 or later, or TLS 1.0 or later, to be enabled in your web browser. Otherwise, the browser displays an error indicating that the page cannot be displayed. We recommend the higher security options of SSL 3.0 or the latest TLS if it is available.

4. When the login dialog box appears, provide the required Username and Password credentials.

   Typically, you log in with the Linux root user name and password.

5. Use the links in Novell Remote Manager to view, configure, and manage the server.

   For information about navigating in Novell Remote Manager, see Section 6.4, "Understanding the Layout of Novell Remote Manager," on page 24.

6. After your session for Novell Remote Manager is complete, click the Exit icon to log out, then close the web browser.

   After you log in, your session for Novell Remote Manager remains open until you log out or close your web browser. There is no automatic time-out period that triggers a logout. For security reasons, you should also close the browser windows at that workstation after you log out.
6.3 **Starting or Stopping HTTPSTKD**

When you install and configure the Novell Remote Manager pattern on Open Enterprise Server (OES) server, Novell Remote Manager is started by default.

A script for starting and stopping the Novell Remote Manager/Linux components is in /etc/init.d/novell-httpstkd. Enter the following commands at a console shell prompt to perform the desired action:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To see whether the module is running</td>
<td>rcnovell-httpstkd status</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>/etc/init.d/novell-httpstkd status</td>
</tr>
<tr>
<td>To restart HTTPSTKD</td>
<td>rcnovell-httpstkd restart</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>/etc/init.d/novell-httpstkd restart</td>
</tr>
<tr>
<td>To start HTTPSTKD</td>
<td>rcnovell-httpstkd start</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>/etc/init.d/novell-httpstkd start</td>
</tr>
<tr>
<td>To stop HTTPSTKD</td>
<td>rcnovell-httpstkd stop</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>/etc/init.d/novell-httpstkd stop</td>
</tr>
</tbody>
</table>

6.4 **Understanding the Layout of Novell Remote Manager**

The web pages for Novell Remote Manager have three main frames: the header frame (top), the navigation frame (left), and the main content frame (right). They also contain the Overall Health Indicator and online help.

Figure 6-1 on page 25 shows the overall layout of Novell Remote Manager for OES 2015 SP1. Figure 6-2 on page 26 shows the overall layout of Novell Remote Manager for OES 11 SP1 and earlier. For OES 2015 SP1, the key additions are the Novell CIFS plug-in to manage CIFS connections and the Novell AFP plug-in to manage AFP connections. Under the Diagnose option, the Health Monitor function is obsoleted by the use of Ganglia and Nagios open source software to monitor system performance and services health. The overall health status displayed in the header frame is based on the status of services monitored on the Nagios Service Detail page.
Figure 6-1  Layout of Novell Remote Manager for OES 11 SP2 and Later
Figure 6-2  Layout of Novell Remote Manager for OES 11 SP1 and Earlier

See the following sections for more information about the layout of the Novell Remote Manager Home page:

- Section 6.4.1, “Header Frame,” on page 27
- Section 6.4.2, “Overall Health Indicator,” on page 27
- Section 6.4.3, “Navigation Frame,” on page 28
- Section 6.4.4, “Program Plug-Ins in the Navigation Frame,” on page 29
- Section 6.4.5, “Main Content Frame,” on page 29
- Section 6.4.6, “Online Help,” on page 29
6.4.1 Header Frame

The header frame contains the toolbar and general information about the server.

The toolbar buttons link to the following functions:

- **Home**
  The File System Management page is considered the Home page.

- **Exit**
  Log out of your current session with Novell Remote Manager. For security reasons, you should also close the web browser Window.

- **Health Monitor** (Nagios Service Detail in OES 11 SP2 and later)
  For information about configuring and using Nagios to monitor services, see Section 8.5, “Configuring Nagios,” on page 47.

- **Configuration**
  For information about Novell Remote Manager Configuration Options, see Chapter 7, “Changing the HTTPSTKD Configuration,” on page 31.

The general information about the server includes the following:

- Name of the user you logged in as to Novell Remote Manager (typically, the root user)
- Overall health indicator
- Server hostname
- Version of the Linux kernel running on the server
- Hardware platform
- Operating system running on the server
- Up time for the server (the amount of time the server has been running since the last reboot) in the format of days:hh:mm:ss.

You can also access Novell Support (http://www.novell.com/support) by clicking the Novell big red N icon on the right side of the header frame.

6.4.2 Overall Health Indicator

The Overall Health Indicator shows the current server health status as good, suspect, bad, or no connection. For OES 2015 SP1, the status is determined from the services that you configure to be monitored by Nagios. The indicator changes if any Nagios-monitored service has a problem alert. If there are multiple alerts, the indicator represents the worst reported health condition. You can click the Server Health icon (shown in Table 6-2) to go to the Nagios Service Detail page and view the health statistics and alerts for the monitored services. By default, only basic services are set up to be monitored by Nagios. In order for the Overall Health Indicator to consider the health of additional services, you must configure them to be monitored by Nagios. For information about configuring and using Nagios, see Section 8.5, “Configuring Nagios,” on page 47.
Table 6-2 Overall Server Health Status Conditions

<table>
<thead>
<tr>
<th>Overall Health Status</th>
<th>Server Health Icon</th>
<th>Icon Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>![Green orb in a white circle]</td>
<td>Green orb in a white circle</td>
</tr>
<tr>
<td>Suspect</td>
<td>![Yellow diamond in a white circle]</td>
<td>Yellow diamond in a white circle</td>
</tr>
<tr>
<td>Bad</td>
<td>![Red bar in a white circle]</td>
<td>Red bar in a white circle</td>
</tr>
<tr>
<td>No connection to the server</td>
<td>![Black X in a white circle]</td>
<td>Black X in a white circle</td>
</tr>
</tbody>
</table>

6.4.3 Navigation Frame

The navigation frame lists general tasks that you can perform, and provides links to specific pages for performing those tasks. The left navigation frame includes collapsible categories that are remembered the next time you log in. This lets you display the Novell Remote Manager features that you use most often and hide some of the ones that you don't.

**IMPORTANT:** When you work in Novell Remote Manager, you must use the navigation links provided in the tool. Using the browser's Back button can result in unintended actions being re-sent to the server.

Basic links in the navigation frame are identified in Table 6-3.

Table 6-3 Standard Roles in the Navigation Frame

<table>
<thead>
<tr>
<th>Roles</th>
<th>Description</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnose</td>
<td>Monitor the health of the server and services.</td>
<td>Chapter 8, “Diagnosing Problems Using Ganglia and Nagios (OES 2015 SP1),” on page 39</td>
</tr>
<tr>
<td>View File System</td>
<td>Browse the file system, view information about files, folders, and partitions, and generate inventories.</td>
<td>Chapter 9, “Viewing File Systems,” on page 63</td>
</tr>
<tr>
<td>Manage Linux</td>
<td>View information about kernel modules, packages, and processes. Schedule CRON jobs.</td>
<td>Chapter 10, “Managing Linux,” on page 71</td>
</tr>
<tr>
<td>Manage Hardware</td>
<td>View information about processors, interrupts, memory, ports, and SMBIOS.</td>
<td>Chapter 11, “Managing Hardware,” on page 81</td>
</tr>
<tr>
<td>Use Group Operations</td>
<td>Configure groups of servers to be monitored collectively.</td>
<td>Chapter 12, “Using Group Operations,” on page 87</td>
</tr>
</tbody>
</table>
6.4.4 Program Plug-Ins in the Navigation Frame

The links in the navigation frame change depending on the programs installed on the server that have plug-ins to Novell Remote Manager. The plug-ins are installed automatically when you install the related OES Services.

<table>
<thead>
<tr>
<th>OES Service</th>
<th>Roles in the Navigation Frame</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCP Server and Dynamic Storage Technology</td>
<td>Manage NCP Services allows you to manage NSS volumes, NCP volumes, DST volumes, NCP volume inventories, and NCP connections on the server.</td>
<td>Chapter 13, “Managing NCP Services,” on page 99</td>
</tr>
<tr>
<td></td>
<td>Dynamic Storage Technology Options allows you to configure and manage Dynamic Storage Technology volumes and policies. The DST functions are integrated with Manage NCP Services.</td>
<td>Chapter 14, “Managing Dynamic Storage Technology Options,” on page 127</td>
</tr>
<tr>
<td>Novell CIFS</td>
<td>Manage CIFS Services allows you to manage Novell CIFS connections on the server.</td>
<td>Chapter 15, “Managing CIFS Services,” on page 131</td>
</tr>
<tr>
<td>Novell AFP</td>
<td>Manage AFP Services allows you to manage Novell AFP connections on the server.</td>
<td>Chapter 16, “Managing AFP Services,” on page 135</td>
</tr>
</tbody>
</table>

6.4.5 Main Content Frame

The information in the main content frame changes depending on which link you click in the header or navigation frame. The File System Management page is considered the Home page.

6.4.6 Online Help

When a Help icon appears in the upper-right corner of a page in the main content frame, you can view help for the page that is displayed.

6.5 Accessing Configuration Options

Click the Configure icon in the header frame to access the Configuration Options page. Use this page to configure the following:

- HTTP Interface Management
- Nagios Configuration Options (only for OES 11 SP2 and later)
6.6 Accessing Online Help

Online help, which provides detailed information and instructions for using Novell Remote Manager features, is available for most management tasks and settings.

To access the online help, click the Help icon on the upper right portion of the page or next to the specific item link.

6.7 Accessing Novell Web Pages

Novell Links on the Home (File System Management) page provide quick access to the following:

- Novell Support (http://www.novell.com/support/) links directly to the Novell Support website, where you can get current server patch kits and updates or find troubleshooting information.

  You can also access Novell Support by clicking the Novell big red N icon on the right side of the header frame.

- Novell Error Codes (http://www.novell.com/documentation/nwec/index.html) links directly to the information about Novell Error Codes, including what they mean and possible causes and actions for them.

- Novell Product Documentation (http://www.novell.com/documentation) links directly to the product documentation for all shipping Novell products.

- Novell Developer Support (http://www.novell.com/developer/) links directly to the Novell Developer website, where you can find tips and suggestions beyond the basics for managing, troubleshooting, and diagnosing your server.
Changing the HTTPSTKD Configuration

When Novell Remote Manager (NRM) is installed, it sets up a small web server on your server. The interface and module is called HTTPSTKD. It automatically sets its basic configuration parameters that allow it to work.

You might need to configure Novell Remote Manager after the initial installation for a variety of reasons. For example, you might want to bind additional IP addresses to HTTPSTKD, set up stronger security, or extend the eDirectory schema for Group Monitoring.

You can perform these tasks using the options on the Novell Remote Manager Configuration Options page, as shown in Figure 7-1. To access this page, click the Configure icon in the header frame.

For OES 2015 SP1, the Configuration Options page also provides links for Nagios Configuration Options. For information about changing the Nagios configuration, see Section 8.5, “Configuring Nagios,” on page 47.
## Novell Remote Manager Configuration Options

### HTTP Interface Management

**WARNING:** You must restart httpstkd in order to apply changes in these config files.

- Edit `httpstkd.config` file
- Edit `httpstkd.PAM.config` file

### Nagios Configuration Options

- Edit `nagios.cfg` file
- Edit `nagios command cfg` file
- Edit `nagios config` file
- Edit `nagios object command config` file
- Edit `nagios object contact config` file

### Nagios User Management

- Restart Nagios

### Daemon Restart

- Restart `httpstkd`

### HTTP Logs

- View last 100 log entries
- View entire log

### Novell Remote Manager Certificate Management

*httpstkd has been configured to use the YAST CA certificate.*

- Create an OpenSSL Certificate and configure httpstkd to use the OpenSSL Certificate
- Enable access using SSLv2 Certificates

### Novell Remote Manager Schema Management

*Disabled:* You must be logged in as a eDirectory user with admin rights to apply Novell Remote Manager schema extensions.

### httpstkd Daemon Core File: Enabled

**Current Working Directory:** `/opt/novell/httpstkd/sbin`

- Disable

On this page you can perform the following tasks:

- Section 7.1, “Accessing and Editing the HTTPSTKD Configuration File,” on page 33
- Section 7.2, “Accessing and Editing the HTTPSTKD PAM Configuration File,” on page 34
- Section 7.3, “Restarting the HTTPSTKD Daemon,” on page 35
- Section 7.4, “Viewing the HTTP Logs,” on page 35
- Section 7.5, “Viewing and Creating Certificates for Novell Remote Manager,” on page 35
- Section 7.6, “Extending the eDirectory Schema for Novell Remote Manager Group Operations,” on page 37
7.1 Accessing and Editing the HTTPSTKD Configuration File

Anytime you want to change the functionality of Novell Remote Manager, access the `/etc/opt/novell/httpstkd.conf` file, modify the settings, then restart the HTTPSTKD daemon.

To access and edit this file from within Novell Remote Manager:

1. Log in to Novell Remote Manager as the root user.
2. Click the Configure icon in the navigation frame.
3. Click Edit httpstkd config file.
4. Make the changes.
5. Click Save Changes.

You can alternatively open the `/etc/opt/novell/httpstkd.conf` file in a text editor that saves files to a UNIX format, edit the file, then save the file.

After making changes to this file and saving it, restart the HTTPSTKD daemon. See “Restarting the HTTPSTKD Daemon” on page 35. You can also restart it manually as described in Section 6.3, “Starting or Stopping HTTPSTKD,” on page 24.

Table 7-1 identifies the functions that are controlled by settings in the Novell Remote Manager configuration file, and provides links to information about how to change them.

### Table 7-1: Information for Changing the Functionality of Novell Remote Manager

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Information about How to Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which network adapter Novell Remote Manager is bound to or add additional IP address that it is bound to</td>
<td>Section A.1, “Address and Port Commands,” on page 153</td>
</tr>
<tr>
<td>The certificates Novell Remote Manager is using for authentication</td>
<td>• Section 7.5, “Viewing and Creating Certificates for Novell Remote Manager,” on page 35</td>
</tr>
<tr>
<td></td>
<td>• Section A.1, “Address and Port Commands,” on page 153</td>
</tr>
<tr>
<td>The cipher strength of the SSL key that is used to access Novell Remote Manager</td>
<td>Section A.9, “SSL Key Cipher Strength Command,” on page 162</td>
</tr>
<tr>
<td>The HttpOnly attribute for cookies in a response header</td>
<td>Section A.5, “HttpOnly Command,” on page 158</td>
</tr>
<tr>
<td>The <code>InventoryResolveNonLumOwnerName</code> option for resolving names of NSS volume file owners if their eDirectory user names are not LUM enabled</td>
<td>Section A.6, “InventoryResolveNonLumOwnerName Command,” on page 159</td>
</tr>
<tr>
<td>Which plug-ins are loaded</td>
<td>Section A.8, “Load Command,” on page 161</td>
</tr>
<tr>
<td>Which workstations can access Novell Remote Manager</td>
<td>Section A.4, “Filtering Commands,” on page 157</td>
</tr>
<tr>
<td>For OES 11 SP1 and earlier, whether an email notification is sent for the Health Monitor tool or who receives it</td>
<td>Section A.3, “Email Notification Commands (OES 11 SP1 and Earlier),” on page 156</td>
</tr>
</tbody>
</table>
7.2 Accessing and Editing the HTTPSTKD PAM Configuration File

Linux uses PAM (Pluggable Authentication Modules) in the authentication process as a layer that mediates between user and application. PAM modules are available on a system-wide basis, so they can be requested by any application.

Every program that relies on the PAM mechanism has its own configuration file in the directory `/etc/pam.d/program_name`. These files define the PAM modules that are used for authentication. In addition, there are global configuration files for most PAM modules under `/etc/security` directory, which define the exact behavior of these modules (examples are `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf`, and `time.conf`). Every application that uses a PAM module actually calls a set of PAM functions, which then processes the information in the various configuration files and returns the results to the calling application.

This file controls the authentication to Novell Remote Manager on an OES Linux server. The default configuration should work. If you want to change the way your users authenticate to Novell Remote Manager, you can edit this file.

These are the lines that enable Novell Remote Manager integration with user management:

```
auth   sufficient pam_nam.so
account sufficient pam_nam.so
password sufficient pam_nam.so
session optional   pam_nam.so
```

To access and edit this file from within Novell Remote Manager:

1. Log in to Novell Remote Manager as the root user.
2. In Novell Remote Manager, click the Configure icon in the navigation frame.
3. Click Edit httpstkd PAM config file.
4. Make the changes.
5. Click Save Changes.
6. After making changes to this file, restart the HTTPSTKD daemon. See “Restarting the HTTPSTKD Daemon” on page 35.

You can alternatively use an editor that saves files to a UNIX format to edit the `/etc/pam.d/httpstkd` file. After changing the file, restart the HTTPSTKD daemon. See “Restarting the HTTPSTKD Daemon” on page 35.

7.3 **Restarting the HTTPSTKD Daemon**

After making changes to the HTTPSTKD configuration file or the HTTPSTKD PAM configuration file, restart the HTTPSTKD daemon.

To restart the HTTPSTKD daemon, click **Restart httpstkd** on the Novell Remote Manager Configuration Options page.

You can also restart it manually. See "Starting or Stopping HTTPSTKD" on page 24.

7.4 **Viewing the HTTP Logs**

The Novell Remote Manager Configuration Options page contains a link for all the HTTPSTK-related messages contained in the `/var/log/messages` file.

This information is valuable for seeing who logged in through Novell Remote Manager, when they logged in, the pages being viewed, log failures, and so on.

You can view the last 100 entries of the log or the entire log.

To view this log:

1. Click the **Configure** icon in the navigation frame.
2. Under the **HTTP Logs** heading, click either **View last 100 log entries** or **View entire log**.

The logging to this file is controlled by the Syslog options. To change these default syslog options, edit the `etc/sysconf/syslog` file.

7.5 **Viewing and Creating Certificates for Novell Remote Manager**

Novell Remote Manager uses the default certificates created during the installation to secure access through it to the server. This certificate is bound to the first network board found in the server configuration.

During the install of eDirectory on a new server installation, there is a check box to have all HTTP services use an eDirectory certificate. HTTPSTKD uses that certificate if this check box is selected or the YAST CA certificate if it is not selected. On upgrades, the check box in eDirectory is not selected, so certificates that were previously used are maintained.

You can create new certificates and modify the `/etc/opt/novell/httpstkd.conf` file to use any certificates other than the default certificate file for any reason. You should create a new certificate in cases such as the following:

- The default certificate does not meet the level of security required by your organization
- The default certificate was bound to a DHCP address
- You have changed the server’s IP address
- You want to bind a new certificate to a different network board
To view the certificates being used:

1. Click the **Configure** icon in the navigation frame.
2. Under the **Novell Remote Manager Certificate Management** heading, click **View Certificate(s)**.

To create a new certificate:

1. Click the **Configure** icon in the navigation frame.
2. Under the **Novell Remote Manager Certificate Management** heading, click **Create Certificate**.
3. On the Create a Certificate for Novell Remote Manager page, specify the required information in the **Certificate Information** fields.
   This creates a new certificate and automatically replaces the current certificate at `/etc/opt/novell/httpstkd/server.pem`.
   If you want to create the certificate in a different location or with a different name, change the file name or path in the **Certificate File** field.
4. Click **Create**.
5. (Conditional) If you changed the name of the certificate file or the path to it from the default location, edit the `/etc/opt/novell/httpstkd.conf` before restarting HTTPSTKD.
6. Restart HTTPSTKD by clicking the **Restart Httpstkd** button on the Novell Remote Manager Configuration Options page.

To bind Novell Remote Manager to an additional IP address to or to a different certificate:

1. Click the **Configure** icon in the navigation frame.
2. Click **Edit Httpstkd Config File**.
3. In the Address and Port portion of the file, specify the new IP address or certificate path and name.
   For example, if you had two network boards that you wanted to bind Novell Remote Manager to, you would create or have two separate certificates and then make these entries in the `/etc/opt/novell/httpstkd.conf` file:
   ```
   addr 192.27.1.123:8008
   addr 192.27.1.123:8009 keyfile=/etc/opt/novell/httpstkd/server.key certfile=/etc/opt/novell/httpstkd/server1.pem
   addr 192.27.1.124:8008
   addr 192.27.1.124:8009 keyfile=/etc/opt/novell/httpstkd/server.key certfile=/etc/opt/novell/httpstkd/server2.pem
   ```
   You can put the certificate in any location as long as the entry in the `/etc/opt/novell/httpstkd.conf` points to the correct location and file name.
7.6 Extending the eDirectory Schema for Novell Remote Manager Group Operations

When you use Group Operations and want to save the groups that you have created, Novell Remote Manager requires you to save the file on the server locally or assign it to an eDirectory object.

Before you can save it to an eDirectory object, you must extend the eDirectory schema to access the attributes for Novell Remote Manager group operations at least once in the eDirectory tree that you are saving to.

You can do this easily by clicking either the Extend eDirectory Schema for Group Operations link on the Novell Remote Manager Configuration Options page any time before you create a group or the link in the failure error message displayed when saving the group. As with all schema extensions, you must have the necessary rights to extend the schema.

The message NDS schema extension complete is displayed on this page when the operation is done. Then you can save the group.
Novell Remote Manager includes several tools to assist you in monitoring the health and status of your server and services. Beginning in Open Enterprise Server (OES) 2015 SP1, Novell Remote Manager uses the open source monitoring tools Ganglia and Nagios to monitor the health of the server and the services and applications running on it. The tools provide complementary health monitoring functions. Ganglia gathers server metrics and tracks trends over time. Nagios monitors health and provides an alert and notification system. You can use these tools to become familiar with the normal health and status of your server. They can help you identify and diagnose problems with your server.

**IMPORTANT:** The Health Monitor function in Novell Remote Manager is obsoleted in OES 2015 SP1. It is replaced by the Ganglia and Nagios open source monitoring tools, which do not use the Small Footprint CIM Broker (SFCB) for communications.

Performing the following tasks can help you to become familiar with the health and status of your servers:

- Section 8.1, “Monitoring Server Health,” on page 39
- Section 8.2, “Configuring Ganglia,” on page 41
- Section 8.3, “Stopping and Starting Ganglia gmond and gmetad,” on page 44
- Section 8.4, “Monitoring Server Health with Ganglia,” on page 44
- Section 8.5, “Configuring Nagios,” on page 47
- Section 8.6, “Monitoring Service Health with Nagios,” on page 54
- Section 8.7, “Restarting Nagios,” on page 55
- Section 8.8, “Managing Nagios Users,” on page 55
- Section 8.9, “Modifying the Nagios Notification Methods for Contacts,” on page 58
- Section 8.10, “Configuring Nagios Logging,” on page 58
- Section 8.11, “Viewing the PIDs or Monitoring the Health of Processes,” on page 60
- Section 8.12, “Monitoring or Killing an Individual Process,” on page 61
- Section 8.13, “Troubleshooting a Suspect or Bad Health Status,” on page 62

### 8.1 Monitoring Server Health

Monitoring the health of your server can help prevent it from getting to a state in which your users cannot access the server or the data on it. Novell Remote Manager allows you to monitor the server’s overall health and the health of a specific item.

- Section 8.1.1, “Viewing the Overall Server Health Status,” on page 40
- Section 8.1.2, “Setting the Health Status Refresh Rate,” on page 40
8.1.1 Viewing the Overall Server Health Status

The server’s overall health is indicated by the color of the circle displayed next to the Server icon in the header frame for Novell Remote Manager. The following table lists and explains each health status that might be displayed.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Server Health Status</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>Good</td>
<td>All parameters included in the server’s health configuration list are good.</td>
</tr>
<tr>
<td>🟠</td>
<td>Suspect</td>
<td>The status of one or more of the parameters included in the server’s health configuration list is suspect or has a minor problem.</td>
</tr>
<tr>
<td>🔴</td>
<td>Bad</td>
<td>The status of one or more of the parameters included in the server’s health configuration list is bad or has a critical problem.</td>
</tr>
<tr>
<td>🗑</td>
<td>Lost connection</td>
<td>The connection to the server from Novell Remote Manager has been lost.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 8-1 Server Health Status</th>
</tr>
</thead>
</table>

The server’s overall health is determined by services that you configure to be monitored by Nagios.

If the status of any Nagios-monitored service changes to yellow (suspect) or red (bad), the health status indicator light in the header frame changes to indicate there is a problem. If more than one item changes, the worst status indicates the server’s overall status. When the status for all items returns to green (good), then the health light indicator changes back to green (good).

8.1.2 Setting the Health Status Refresh Rate

The server’s health status, reported by the health status indicator, is updated every five seconds, but the graphic refreshes only if the status changes.

- To modify the refresh rate, select a rate from the Page Refresh Rate drop-down menu, then click Begin Refresh. The selected refresh rate applies to this page only, and persists until you modify the value.
- To stop refreshing the page, select Stop Refresh. The page does not refresh until you click Begin Refresh.
- To begin refreshing after stopping, select Begin Refresh. The last used refresh rate is applied automatically when it begins.
8.2 Configuring Ganglia

Ganglia is an open source monitoring tool that collects server metrics and graphically displays their trends over the past hour, day, week, month, or year. It shows similar graphs for memory usage, disk usage, network statistics, number of running processes, and all other Ganglia metrics. The Ganglia Monitoring daemon (gmond) has a low overhead and does not impact user performance.

The Ganglia UI has embedded help to guide you in using the services on each tab. For additional information, see Ganglia Monitoring System (http://ganglia.info) on the web.

- Section 8.2.1, “Ganglia Requirements,” on page 41
- Section 8.2.2, “Configuring Ganglia gmond in Multicast Mode or Unicast Mode,” on page 42

8.2.1 Ganglia Requirements

Ganglia requires the following settings in order to display the server health statistics:

- “Port 8649” on page 41
- “Time Synchronization” on page 41

Port 8649

If a firewall is enabled on the server, you must open port 8649 in order to use Ganglia. By default, the gmond daemon communicates on UDP port 8649, and the gmetad daemon downloads metrics data over TCP port 8649. The port is specified in udp_send_channel, udp_recv_channel, and tcp_accept_channel parameters in the /etc/opt/novell/ganglia/monitor/gmond.conf file. If you have firewall rules that block traffic on those ports, your metrics do not show up in the monitoring dashboard. You must restart the Ganglia gmond and gmetad daemons after you open the port in the firewall.

1. Log in to the server as the Linux root user, then open a terminal console.

2. Open port 8649 in the firewall. Enter
   
   SuSEfirewall2 open EXT UDP 8649
   SuSEfirewall2 open EXT TCP 8649

3. Restart gmond and gmetad. Enter
   
   rcnovell-gmond stop
   rcnovell-gmetad stop
   rcnovell-gmetad start
   rcnovell-gmond start

Time Synchronization

If your Ganglia server monitors the health of multiple computers, ensure that the time on the gmond server is correct and matches the gmetad that is collecting data. The timestamp used to update the gmetad round-robing database (RRD) files are in the Universal Time Coordinated (UTC) standard, which is the international time standard.

Consider using the same Network Time Protocol (NTP) time source on the group of machines in order to keep their time synchronized. NTP is an industry standard. It ensures accurate timekeeping by synchronizing clocks to UTC time. If a firewall is enabled on the servers, ensure that you open the
firewall on UDP port 123 to allow NTP traffic. After you configure NTP, delete the current gmetad round-robin databases (RRDs) in the /var/opt/novell/ganglia/rrds subdirectories, and then restart gmond and gmetad.

1. Log in to the server as the Linux root user, then open a terminal console.
2. Open port 123 in the firewall. Enter
   ```
   SuSEfirewall2 open EXT UDP 123
   ```
3. Configure NTP on the server.
   For information about configuring NTP, see “Time Services” in the OES 2015 SP1: Planning and Implementation Guide.
4. In a file browser, delete the current gmetad round-robin databases (RRDs) in the /var/opt/novell/ganglia/rrds directory.
5. Restart gmond and gmetad. Enter
   ```
   rcnovell-gmond stop
   rcnovell-gmetad stop
   rcnovell-gmetad start
   rcnovell-gmond start
   ```

### 8.2.2 Configuring Ganglia gmond in Multicast Mode or Unicast Mode

Ganglia uses the gmond daemon to gather health monitoring statistics. It keeps a cache of all metrics in memory. Ganglia uses the gmetad daemon to periodically poll the gmond daemon to store the metrics in a storage engine. By default, Novell Remote Manager configures Ganglia in multicast mode. Both the gmond daemon and the gmetad run on the same server.

The gmond daemon can alternatively be configured in unicast mode. You can also configure it to monitor in groups of servers, called Ganglia clusters. For more information, see the Ganglia Quick Start Guide (http://sourceforge.net/apps/trac/ganglia/wiki/ganglia_quick_start) on the Ganglia Project website.

- “Using Ganglia in Multicast Mode” on page 42
- “Using Ganglia in Unicast Mode” on page 43
- “Configuring gmond for Server-Centric Monitoring” on page 43

### Using Ganglia in Multicast Mode

By default, the Ganglia gmond daemon is configured in multicast mode, and that is how it is installed for Novell Remote Manager. Ganglia settings for gmond are in the /etc/opt/novell/ganglia/monitor/gmond.conf file.

The gmond daemon’s global parameters are set for it to be both a sender (mute=no) and a receiver (deaf=no). The gmond daemon aggregates all metrics sent to it from other hosts running Ganglia in the same IP subnet, or in the same Ganglia cluster (if configured). There is no need to list every single host, because a gmond set in receive mode automatically contains the list of all hosts and metrics in the subnet (or in the same Ganglia cluster, if configured). Metrics and their metadata (metric groups, types and so on) are sent separately. If Ganglia is restarted while using multicast mode, gmond servers can talk to each other, and will ask for metadata if it is missing.
Ganglia settings for gmetad are in the `/etc/opt/novell/ganglia/monitor/gmetad.conf` file. Its root directory for the round-robin databases (RRDs) is the `/var/opt/novell/ganglia/rrds` directory. The data source for the localhost is named Grid-Node, and its metrics RRD files are found in the `/var/opt/novell/ganglia/rrds/Grid-Node` directory.

You can turn off multicasting to view statistics only for the single server where you are logged in to Novell Remote Manager. For more information, see “Configuring gmond for Server-Centric Monitoring” on page 43.

### Using Ganglia in Unicast Mode

Unicast mode has less traffic than multicast mode does, but it is more complex to configure. In unicast mode, the default behavior for handling metadata is as follows:

- The gmond daemon sends metadata only when it is started.
- If Ganglia is restarted while using unicast mode, metadata is discarded and its corresponding metrics data are also discarded.
- Ganglia does not ask for metadata if it is missing.

The unicast behavior might result in blank graphs on the host-view page if the collecting gmond is restarted while working in unicast mode. Restarting all of the non-collector gmond daemons makes the metric graphs reappear; however, this might not be feasible for large Ganglia clusters. If you use the unicast mode to monitor multiple servers, you should enable the global parameter `send_metadata_interval` in the `/etc/opt/novell/ganglia/monitor/gmond.conf` file, and set it to something other than 0. A setting of 30 to 60 seconds works in most environments. Setting this variable to a non-zero value makes the gmond processes periodically announce their metrics, and the graphs reappear on the host-view page.


### Configuring gmond for Server-Centric Monitoring

You can modify the `/etc/opt/novell/ganglia/monitor/gmond.conf` file to set up Ganglia to monitor only its own statistics as a single server.

1. Log in to the server as the `root` user.
2. Open the `/etc/opt/novell/ganglia/monitor/gmond.conf` file in a text editor.
3. Find the section `udp_send_channel` and replace it with the following:

   ```
   udp_send_channel {  
       #bind_hostname = yes  
       mcast_join = 239.2.19.61  
       port = 8649  
       #ttl = 1  
   }
   
   You comment out the `mcast_join` parameter and the `ttl` parameter.

   4. Find the section `udp_recv_channel` and replace it with the following:

   ```
   udp_recv_channel {  
       #mcast_join = 239.2.19.61  
       port = 8649  
       #bind = 239.2.19.61  
   }"
You comment out the `mcast_join` parameter and the `bind` parameter.

5 Save and close the file.

6 Open a terminal console, and then stop and start both `gmond` and `gmetad`:

```bash
rcnovell-gmond stop
rcnovell-gmetad stop

rcnovell-gmetad start
rcnovell-gmond start
```

### 8.3 Stopping and Starting Ganglia gmond and gmetad

1 Log in to the server as the Linux `root` user, then open a terminal console.

2 Restart gmond and gmetad. Enter

```bash
rcnovell-gmond stop
rcnovell-gmetad stop

rcnovell-gmetad start
rcnovell-gmond start
```

### 8.4 Monitoring Server Health with Ganglia

The **Diagnose > Server Health Values** task presents the Ganglia Web interface in the Novell Remote Manager browser frame. You can use this page to monitor your server’s health statistics. The Ganglia UI has embedded help to guide you in using the services on each tab. For additional information, see [Ganglia Monitoring System](http://ganglia.info) on the web.

1 Access the Ganglia dashboard, using one of the following methods:

   - Log in to Novell Remote Manager as the Linux `root` user or as a LUM-enabled administrator user.

   - Select **Diagnose > Server Health Values** to go to the Ganglia main dashboard. Continue to **Step 2 on page 45**.

   or

   - In a web browser, go to the Ganglia URL:

     ```bash
     http://<server_ip_address>/gweb
     ```
2 If you are prompted with a security warning that the page contains mixed content (both secure and non-secure elements), select the option to show all content.

The Novell Remote Manager frame sends secure content. However, Ganglia uses scripts to graphically display statistics that send the statistical data via HTTP instead of HTTPS. Depending on how your web browser is configured to handle mixed content on a web page, the Ganglia statistics might not be displayed in the graph windows.

- Firefox: In Firefox 23 and later, when you access a page with both HTTPS and HTTP content, a shield icon 🏷 appears in the address bar, and the browser automatically blocks certain content such as non-secure scripts. To allow mixed content, right-click the shield icon, then select Disable Protection on This Page. After you disable protection, an orange alert icon ⚠ appears in the address bar and makes you aware that the displayed page contains mixed content.
In a Mozilla Firefox 22 and earlier web browser, you receive a warning, but content is not automatically blocked. A Security Warning pop-up dialog box reports: You have requested an encrypted page that contains some unencrypted information. Click OK to dismiss the warning and allow mixed content to be displayed.

A round shield icon replaces the lock to the left of the https:// in the address bar. Right-click the icon to view the message that advises: Your connection to this site is only partially encrypted, and does not prevent eavesdropping.

- **Internet Explorer:** In a Microsoft Internet Explorer web browser, the pop-up dialog box is displayed at the bottom of the page and reports: Only secure content is displayed. Click Show all content to dismiss the warning and allow mixed content to be displayed.

- **Chrome:** In a Google Chrome web browser, a shield appears at the end of the URL in the address bar. It warns: This page includes scripts from unauthenticated resources. Right-click the shield, then click Load Unsafe Script.

While mixed content is displayed in Chrome, the green text https:// and lock in the URL, which indicates secure-only content, is automatically changed to red text that is crossed out and a gray lock with a red X.
Select any of the following tabs to search, configure events to monitor, or define reports:

- Search
- Views
- Aggregate Graphs
- Compare Hosts
- Events
- Automatic Rotation
- Live Dashboard
- Mobile

8.5 Configuring Nagios

Nagios is an open source monitoring tool. You can configure it to monitor the health of the server systems and services. It also provides an alert and notification system.

The information in this section provides basic information to get you started using Nagios. For detailed information about configuring and using Nagios to monitor your server and services, see other sections in this guide. See also the open source Nagios Documentation (http://www.nagios.org/documentation) at Nagios.org.

- Section 8.5.1, "Configuring Nagios Authenticated Users and Contacts," on page 47
- Section 8.5.2, "Configuring Nagios Monitoring," on page 51
- Section 8.5.3, "Accessing the Nagios Website," on page 53
- Section 8.5.4, "Using Nagios Plug-Ins," on page 53
- Section 8.5.5, "Using Object Configuration Files," on page 54
- Section 8.5.6, "Additional Information," on page 54

8.5.1 Configuring Nagios Authenticated Users and Contacts

Nagios user accounts are specific to the Nagios software. The accounts have nothing to do with the local server user names or eDirectory user names.

There are two levels of access for Nagios users:

- **Authenticated user**: a Nagios user who is granted access to the web-based Nagios monitoring dashboard.

- **Authenticated contact**: An authenticated Nagios user whose user name is also defined in the Nagios Object Contact configuration file (/etc/nagios/objects/contacts.cfg) and has permissions to access CGI information as defined in the Nagios CGI configuration file (/etc/nagios/cgi.cfg) and other object configuration for services that are monitored.

By default, the Nagios user **nagiosadmin** is already configured in Nagios as a user, a contact, and a member of the contact group **admins**. This user is also authorized to access server and services information and to issue host or service commands via the command CGI configuration file (/etc/
nagios/cgi.cfg). However, you must configure a password for the nagiosadmin user in order to log in to the Nagios Service Details website. You must configure a valid email address for the nagiosadmin contact in order to receive alerts via the Nagios alert notification system.

- “Setting or Modifying the Password for the nagiosadmin User” on page 48
- “Setting or Modifying an Email Address for the nagiosadmin Contact” on page 49
- “Using the Nagios admins Contact Group” on page 51

### Setting or Modifying the Password for the nagiosadmin User

By default, Nagios defines one default user nagiosadmin with no password in the /etc/nagios/htpasswd.users file. Novell Remote Manager requires passwords to be set for any Nagios user. Thus, before you can access the web-based Nagios Service Details report for the first time, you must specify a password to use for the user nagiosadmin.

**IMPORTANT:** Do not delete the nagiosadmin user.

To configure a password for user nagiosadmin:

1. Log in to Novell Remote Manager as the Linux root user.
2. Click the Configure icon in the toolbar to go the Novell Remote Manager Configuration Options page.
4. On the Nagios User Management page, specify nagiosadmin as the Nagios user name.
5. Type a password, then type it again to confirm.
6. Click Create User.

The user name and password are saved in the /etc/nagios/htpasswd.users file. The password is stored in encrypted format. The password is enforced on the next login to Nagios.
7 When a message confirms that the user **nagiosadmin** was created in Nagios with the password you provided, click **OK** to dismiss the message.

### Nagios User Management

<table>
<thead>
<tr>
<th>Nagios User Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>The username <strong>nagiosadmin</strong> was created with the entered password for use in Nagios.</td>
</tr>
</tbody>
</table>

For information about configuring additional Nagios users and the tasks they can perform, see Section 8.8, “Managing Nagios Users,” on page 55.

### Setting or Modifying an Email Address for the nagiosadmin Contact

By default, Nagios defines the **nagiosadmin** user as a contact in the `/etc/nagios/objects/contacts.cfg` file. It sets the email for the contact to nagios@localhost. In order to receive notification alerts from the Nagios alert notification system, you must replace this email setting with a valid email address. You must restart Nagios to apply the changes.

**IMPORTANT:** Do not delete the **nagiosadmin** contact or its email definition line in the `/etc/nagios/objects/contacts.cfg` file.

To configure an email address for the contact **nagiosadmin**:

1. Log in to Novell Remote Manager as the Linux **root** user.
2. Click the **Configure** icon in the toolbar to go to the Novell Remote Manager Configuration Options page.
3. Under **Nagios Configuration Options**, click **Edit Nagios object contact config file**. This opens the `/etc/nagios/objects/contacts.cfg` file in the Novell Remote Manager text editor.
4. Scroll down to the **contact definition section for nagiosadmin**, and then replace nagios@localhost with the email address (such as bob@example.com) where you want to receive alert notifications that are sent to **nagiosadmin**.
5 Click **Save Changes**.

The changes are saved in the `/etc/nagios/objects/contacts.cfg` file. You can verify the new saved date for the file.

6 Click the **Configure** icon in the toolbar to return to the Novell Remote Manager Configuration Options page, then restart Nagios.

6a Under **Nagios Configuration Options**, click **Restart Nagios**.

6b When you are prompted to confirm the restart, click **OK** to proceed.

6c Wait while Nagios is restarted with the `rcnagios restart` utility.

**Nagios Restart**

Nagios is being restarted with the “rcnagios restart” utility.

When the restart is completed, Novell Remote Manager returns to the Configuration Options page.
Using the Nagios admins Contact Group

Nagios defines a default contact group admins and adds the contact nagiosadmin as a member of the group in the contactgroup section of the /etc/nagios/objects/contacts.cfg file.

If you create additional Nagios users and contacts, you can add them to the admins group. It is not necessary to create additional contact groups. However, Nagios also allows you to create other contact groups to make it easier to set up authorizations for Nagios users who have different roles.

**IMPORTANT:** Do not remove the default contact group admins from the /etc/nagios/objects/contacts.cfg file. Do not remove the Nagios contact nagiosadmin from the group admins.

You can set up contacts, contact groups, and members of contact groups in the Nagios Object Contact configuration file on the Novell Remote Manager Configuration Options page (or in the /etc/nagios/objects/contacts.cfg file). You must restart Nagios to apply the changes.

8.5.2 Configuring Nagios Monitoring

Nagios is automatically configured with basic monitoring settings for the server. The Nagios contact nagiosadmin has all the necessary authorizations to manage and use Nagios.

You can also define other Nagios users and set them up as contacts, set the CGI and object authorizations for Nagios contacts, specify the systems and services to monitor, specify display preferences for the dashboard, set up logging preferences, and set up notifications. As the Linux root user, you can go to the Novell Remote Manager Configuration Options > Nagios Configuration Options in order to perform the tasks described in Table 8-2.

**Table 8-2 Nagios Configuration Options**

<table>
<thead>
<tr>
<th>Nagios Configuration Option</th>
<th>Related File or Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Nagios cgi config file</td>
<td>/etc/nagios/cgi.cfg</td>
<td>Defines the CGI parameters and which contacts or contact groups are allowed to access them.</td>
</tr>
<tr>
<td>Edit Nagios command config file</td>
<td>/etc/nagios/command.cfg</td>
<td>Defines commands, including service check, service notification, host check, host notification, service event handler, and host even handler.</td>
</tr>
<tr>
<td>Edit Nagios config file</td>
<td>/etc/nagios/nagios.cfg</td>
<td>Specifies the main log file where service and host events are logged. For more information, see Section 8.10, “Configuring Nagios Logging,” on page 58. You can configure other Nagios parameters as defined in the configuration file.</td>
</tr>
<tr>
<td>Edit Nagios object command config file</td>
<td>/etc/nagios/objects/commands.cfg</td>
<td>Provides you with some sample command definitions that you can reference in host, service, and contact definitions.</td>
</tr>
</tbody>
</table>
Novell Remote Manager provides a text editor to modify the configuration files from the web browser. The configuration options are described in-line in each of the Nagios configuration files. After you modify the configuration files, you must restart Nagios to apply the settings. You can alternatively log in to the server as the Linux root user and use a text editor to modify the configuration files in the /etc/nagios folder.

After you modify the configuration files, you should verify the configuration before you restart Nagios. The Nagios daemon will not start if the configuration contains errors.

To verify your configuration, run Nagios with the -v command line option:

```
/usr/sbin/nagios -v /etc/nagios/nagios.cfg
```

If critical data is missing or wrong, Nagios displays a warning or error message that identifies the line in the configuration file that seems to be the source of the problem. Nagios might print only the first error it encounters to prevent the error from cascading the problem to subsequent settings in the file. If you get an error message, correct the line in the configuration file, then repeat the verification until no errors occur. Warning messages can generally be safely ignored, because they are recommendations and not requirements.
8.5.3 Accessing the Nagios Website

The Nagios website configuration file (/etc/apache2/conf.d/nagios.conf) uses basic authentication by default. Information and passwords are sent in clear text.

**IMPORTANT:** You should access Nagios behind the firewall or via secure channels.

When you click Nagios Service Detail, the monitoring dashboard opens in a pop-up browser window. If the pop-up blocker is enabled for your web browser, ensure that you disable the browser's pop-up blocker for the Nagios website (http://<server_ip_address or localhost>/nagios).

Authentication is required by default. You are prompted to log in. You can log in as the default user nagiosadmin, or create and configure other Nagios users.

To access the Nagios Service dashboard via Novell Remote Manager:

1. Log in to Novell Remote Manager as the Linux root user or as a LUM-enabled administrator user.
2. Select Diagnose > Server Health Services.
3. Click Nagios Service Detail.
4. When you are prompted to authenticate by Nagios Access, specify the user name and password of a Nagios user account, then click OK.

To access Nagios reports via the native Nagios browser view:

1. In a web browser, go to the Nagios URL:
   
   http://<server_ip_address>/nagios

2. When you are prompted to authenticate by Nagios Access, specify the user name and password of a Nagios user account, then click OK.
3. Under Monitoring on the left panel of the server's Nagios home page, click Service Detail.

8.5.4 Using Nagios Plug-Ins

Nagios plug-ins are extensions to Nagios that allow you to monitor hosts, devices, services, protocols, and applications. A plug-in performs a specific type of check and reports the results to Nagios.

The Nagios plug-ins package (nagios-plugins) provides a set of basic system monitoring plug-ins. It also includes plug-in libraries that are used by the basic plug-ins and additional plug-ins. You can also find Nagios plug-ins for a variety of services and applications on the Nagios Exchange (http://exchange.nagios.org/) website. Currently, OES 2015 SP1 does not provide plug-ins specifically designed for OES products and services.

Novell Support for Nagios plug-ins is limited to the plug-ins provided by Novell. For information about using the Nagios basic plug-ins, see the Nagios Plug-ins Documentation (http://www.nagios-plugins.org/doc/index.html) on the Nagios Plug-Ins Project (http://www.nagios-plugins.org/) website. If you use third-party plug-ins or open source plug-ins, you must refer to the providers of those plug-ins for support.

A Nagios plug-in can be compiled binaries (written in programming languages such as C or C++) or executable scripts (such as shell, Perl, or PHP). For information about how to create your own Nagios plug-ins, see the Nagios Plug-in Development Guidelines (http://www.nagios-plugins.org/doc/index.html) on the Nagios Plug-Ins Project (http://www.nagios-plugins.org/) website.
8.5.5 Using Object Configuration Files

Templates for Nagios object configuration files are in the /etc/nagios/objects directory. When you start or restart Nagios, it caches the object definitions in the /var/lib/nagios/objects.cache file. The CGIs read information from the cache file, rather than directly from the object configuration files, in order to prevent inconsistencies that can occur if you modify the configuration files after Nagios starts. Thus, if you modify a configuration file, you must restart Nagios to apply the change.

8.5.6 Additional Information

For detailed information about configuring and using Nagios to monitor your server and services, see the Nagios Documentation (http://www.nagios.org/documentation) at Nagios.org.

For additional information about CGI permissions, see Authentication and Authorization in the CGIs (http://nagios.sourceforge.net/docs/3_0/cgiauth.html) in the Nagios Core documentation.

8.6 Monitoring Service Health with Nagios

The Nagios website allows you to monitor the basic services and the services that you configure Nagios to monitor.

You must set up the credentials for the nagiosadmin user before you can view the Nagios health website. For more information, see Section 8.5.1, "Configuring Nagios Authenticated Users and Contacts," on page 47.

You can also configure other Nagios users. For more information, see Section 8.8, "Managing Nagios Users," on page 55.

To monitor service health with Nagios:

1. Log in to Novell Remote Manager as the Linux root user or as a LUM-enabled administrator user.

2. Access the Nagios Service Detail page, using any of the following methods in Novell Remote Manager:
   - Click the Overall server health status indicator icon 🔄.
   - Click the Health Monitor icon ⬇️ in the header frame.
   - Select Diagnose > Server Health Services.

3. On the Nagios Service Detail page, click the Nagios Service Details link to view the Nagios website.

4. When you are prompted, log in to Nagios using the Nagios credentials for the nagiosadmin user or log in another Nagios user that you have configured as a Nagios contact.

   You remain logged in to the Nagios website until you close the web browser.

   For information about setting up Nagios users, see Section 8.8, "Managing Nagios Users," on page 55.

5. When you are done, close the web browser to log out of the Nagios website.
8.7 Restarting Nagios

To restart Nagios from Novell Remote Manager:

1. Log in to Novell Remote Manager as the Linux root user.
2. Click the Configure icon in the toolbar to go the Novell Remote Manager Configuration Options page.
4. When you are prompted to confirm the restart, click OK to proceed.

5. Wait while Nagios is restarted with the rcnagios restart utility.

To restart Nagios from the command line:

1. Log in to the server as the Linux root user, then open a terminal console.
2. At the command prompt, enter rcnagios restart

8.8 Managing Nagios Users

The Nagios User Management tool allows you to add and delete Nagios users, or re-create users to configure new passwords for them. Before you can access the Nagios website, you must use this tool to set a password for the Nagios user nagiosadmin.

- Section 8.8.1, “Creating or Re-Creating a Nagios User,” on page 55
- Section 8.8.2, “Setting Passwords for Nagios Users,” on page 56
- Section 8.8.3, “Deleting a Nagios User,” on page 56
- Section 8.8.4, “Configuring Nagios Contacts and Notification Methods for Them,” on page 57
- Section 8.8.5, “Configuring Nagios CGI Authorization for Contacts,” on page 57

8.8.1 Creating or Re-Creating a Nagios User

1. Log in to Novell Remote Manager as the Linux root user.
2. Go the Novell Remote Manager Configuration Options page.
4 Specify the user name for a Nagios user.
5 Set the password for the Nagios user. Type a password, then type it again to confirm. Passwords are required by default. You must set a password to ensure that authentication is required to access the Nagios web-based dashboard.
6 Click Create User.
   The user name and password are saved in the /etc/nagios/htpasswd.users file. The password is stored in encrypted format. The password is enforced on the next login to Nagios.
7 If you are creating a new Nagios user, ensure that you configure the contact information for the user and the actions the user is allowed to make. Continue with the following sections:
   ♦ Section 8.8.4, “Configuring Nagios Contacts and Notification Methods for Them,” on page 57
   ♦ Section 8.8.5, “Configuring Nagios CGI Authorization for Contacts,” on page 57

### 8.8.2 Setting Passwords for Nagios Users

You typically set passwords for Nagios users when you create the user names.

To add or modify a password for an existing Nagios user:

1 Log in to Novell Remote Manager as the Linux root user.
2 Go the Novell Remote Manager Configuration Options page.
3 Under Nagios Configuration Options, click Nagios User Management.
4 Specify the user name for an existing Nagios user.
5 Set the password for the user. Type a password, then type it again to confirm.
6 Click Create User.
   The user name and password are saved in the /etc/nagios/htpasswd.users file. The password is stored in encrypted format. The password is enforced on the next login to Nagios.

### 8.8.3 Deleting a Nagios User

Only Nagios users are allowed to access the web-based Nagios dashboard. Do not delete the Nagios user name of a Nagios contact who needs access to the dashboard.

**IMPORTANT:** Do not delete the default Nagios user nagiosadmin.

1 Log in to Novell Remote Manager as the Linux root user.
2 Click the Configure icon in the toolbar to go to the Novell Remote Manager Configuration Options page.
3 Under Nagios Configuration Options, click Nagios User Management.
4 Specify the user name for an existing Nagios user.
5 Ignore the Password and Confirm Password fields.
6 Click Delete User.
   The user name and password are removed from the /etc/nagios/htpasswd.users file. The access is denied on the user’s next login to Nagios.
8.8.4 Configuring Nagios Contacts and Notification Methods for Them

After you create a Nagios user, you should define the user as a Nagios contact, in order to control what that user is allowed to do and see. Define the contact in the Nagios Object Contact configuration file on the Novell Remote Manager Configuration Options page (or in the /etc/nagios/objects/contacts.cfg file). You can use the nagiosadmin definition as a template. You must restart Nagios to apply the changes.

To define a new contact:

1. Log in to Novell Remote Manager as the Linux root user.
2. Click the Configure icon to go to the Novell Remote Manager Configuration Options page.
3. Under Nagios Configuration Options, click Nagios User Management, then create a user name and password for the user.
   For more information, see Section 8.8, "Managing Nagios Users," on page 55.
4. Under Nagios Configuration Options, click Edit Nagios Object Contact configuration.
5. Add a contact definition for the existing user name, and provide a valid email address where you want to receive alert notifications for the user.
6. (Optional) Add other contact methods to the contact definition, such as pager, cell phone, instant message, audio alert, and so on.
7. (Optional) Add the contact name as a member of the contact group admins, or to another contact group that you have defined.
8. Under the editing window, click Save Changes.
9. Configure the contact or the contact group for CGI access.
   For more information, see Section 8.8.5, "Configuring Nagios CGI Authorization for Contacts," on page 57.
10. Under Nagios Configuration Options, click Restart Nagios to apply the changes.

8.8.5 Configuring Nagios CGI Authorization for Contacts

The Nagios CGI settings determine who has access to view monitoring and configuration information, and who can submit commands to the Nagios daemon through the web interface. By default, in the CGI configuration file (/etc/nagios/cgi.cfg), the Nagios contact nagiosadmin has all the necessary authorizations to manage and use Nagios:

- System and process information
- Configuration information
- System and process commands via the Nagios command CGI file (/usr/lib/nagios/cgi/cmd.cgi)
- All hosts information
- All services information
- All host-related commands via the Nagios command CGI file (/usr/lib/nagios/cgi/cmd.cgi)
- All service-related commands via the Nagios command CGI file (/usr/lib/nagios/cgi/cmd.cgi)
You can configure a Nagios contact's authorization settings in the Nagios CGI configuration file on the Novell Remote Manager Configuration Options page (or in the /etc/nagios/cgi.cfg file). The configuration options are described in-line in the configuration file. You must restart Nagios to apply the changes.

### 8.9 Modifying the Nagios Notification Methods for Contacts

The Nagios notifications system is configured by default to send email notifications to the Nagios contact nagiosadmin. You must set the email address to use for nagiosadmin in the Nagios Object Contact configuration file on the Novell Remote Manager Configuration Options page (or in the /etc/nagios/objects/contacts.cfg file). You must restart Nagios to apply the changes. For more information, see “Setting or Modifying an Email Address for the nagiosadmin Contact” on page 49.

If you define other Nagios contacts, you must specify at least one notification method for the contact. In addition to email, Nagios can send notifications via pager, cell phone, instant message, audio alert, and so on. How notifications are sent depends on the notification commands that are defined in your object definition files.

Each host and service definition has a contact_groups option that specifies which contact groups receive notifications for that particular host or service. Contact groups can contain one or more individual contacts. Each member contact receives alert notifications according the method configured in its contact definition.

To configure the notification methods to use for Nagios contacts:

1. Log in to Novell Remote Manager as the Linux root user.
2. Go the Novell Remote Manager Configuration Options page.
3. Under Nagios Configuration Options, click Edit Nagios Object Contact configuration.
4. In each contact definition, use the email parameter to specify a valid email address where you want to receive alert notifications that are sent to them. For example, bob@example.com. You can use other notification parameters in a contact definition to specify alternative notification methods for the contact.
5. Under the editing window, click Save Changes.
6. Under Nagios Configuration Options, click Restart Nagios to apply the changes.

### 8.10 Configuring Nagios Logging

By default, Nagios logs events for the host and services in the /var/log/nagios/nagios.log file. Use the /etc/nagios/nagios.cfg file to control logging for Nagios. For information about logging options, see Table 8-3.

<table>
<thead>
<tr>
<th>Logging Parameter</th>
<th>Description and Logging Options</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>log_file</td>
<td>Specifies the path of the log file, including the file name.</td>
<td>/var/log/nagios/nagios.log</td>
</tr>
<tr>
<td>Logging Parameter</td>
<td>Description and Logging Options</td>
<td>Default Setting</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| log_rotation_method   | Specifies the rotation method that Nagios should use to rotate its main log file, or disables rotation of the log.  
  - n: None, don’t rotate the log  
  - h: Hourly rotation (at the top of the hour, every hour)  
  - d: Daily rotation (at midnight, every day)  
  - w: Weekly rotation (at midnight on Saturday evening)  
  - m: Monthly rotation (at midnight on the evening of the last day of the month) | Rotate the nagios.log file at midnight every day.                                |
| log_archive_path      | Specifies the path of the directory where rotated (archived) log files are stored, if log rotation is enabled. | /var/log/nagios/archives                                                        |
| use_syslog            | Specifies whether to log Nagios messages to the syslog facility as well as to the Nagios main log file.  
  - 1: Enable messages to syslog.  
  - 0: Disable messages to syslog. | Messages are sent to syslog as well as to nagios.log.                           |
| log_notifications     | Specifies whether to log notifications.  
  - 1: Log notifications.  
  - 0: Do not log notifications. | Log notifications.                                                              |
| log_service_retries   | Specifies whether to log service check retries.  
  - 1: Log service check retries.  
  - 0: Do not log service check retries. | Log service retries.                                                            |
| log_host_retries      | Specifies whether to log host check retries.  
  - 1: Log host check retries.  
  - 0: Do not log host check retries. | Log host check retries.                                                         |
| log_event_handlers    | Specifies whether to log host and service event handlers.  
  - 1: Log host and service event handlers.  
  - 0: Do not log host and service event handlers. | Log host and service event handlers.                                            |
8.11 Viewing the PIDs or Monitoring the Health of Processes

To view process information, click Manage Linux > View Process Information. On the Process Information page, you can view a list of active processes. Table 8-4 describes the health information that is reported for each process:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Information</td>
<td>Shows an Information icon. Click the Information icon next to the process name to monitor or kill an individual process.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the process or executable program name.</td>
</tr>
<tr>
<td>Owner</td>
<td>Shows the process owner (the user who started the process).</td>
</tr>
</tbody>
</table>

Table 8-4 Process Health Information
8.12 Monitoring or Killing an Individual Process

On the Process Information page for a selected process, you can view information about the process; issue a SIGTERM, SIGKILL, or SIGHUP signal to kill the process; or send a custom signal. The process information is obtained from the `stat` file that is available for the process ID in the `/proc` directory. Process information can also be retrieved at the command line by using the Linux `top` command.

To view process information, click Manage Linux > View Process Information, then click the name link of the process.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ID (Status)     | Shows the process ID (PID) of the task and the current state of the task. The states are Sleep (S), Running (R), Traced (T), or Zombied (Z). These states are modified by a trailing character as follows:  
|                 | • < indicates a process with a negative nice value.  
|                 | • N indicates a process with a positive nice value.  
|                 | • W indicates a swapped-out process for non-kernel processes.                                                                                        |
| CPU Usage %     | Shows the task’s share of the CPU time since the last screen update, expressed as a percentage of total CPU time per processor.                  |
| Priority        | Shows the priority of the task.                                                                                                                  |
| Run Time        | Shows the total CPU time that the task has used since it started.                                                                               |
| Physical Memory (%) | Shows the amount of physical memory in bytes that the task is using, and the percentage of RAM memory that this represents. The Linux `top` command reports this information in kilobytes. |
| Virtual Memory  | Shows the amount of virtual memory in bytes that the task is using to hold the code, data, and stack space memory. This is the value reported by the Linux `top` command's RSS switch. The Linux `top` command reports this information in kilobytes. |

---

8.12 Monitoring or Killing an Individual Process

On the Process Information page for a selected process, you can view information about the process; issue a SIGTERM, SIGKILL, or SIGHUP signal to kill the process; or send a custom signal. The process information is obtained from the `stat` file that is available for the process ID in the `/proc` directory. Process information can also be retrieved at the command line by using the Linux `top` command.

To view process information, click Manage Linux > View Process Information, then click the name link of the process.

**Table 8-5 Process Information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Name</td>
<td>Shows the process or executable program name.</td>
</tr>
<tr>
<td>Process ID</td>
<td>Shows the process identifier.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the current status of the process. The status can be running, sleeping (an interruptible wait), zombie, D (waiting in uninterruptible disk sleep), T (traced or stopped on a signal), or W for paging.</td>
</tr>
<tr>
<td>Command Line</td>
<td>Shows the actual command line of the executed command to start this process.</td>
</tr>
<tr>
<td>Working Directory</td>
<td>Shows the current working directory of the process.</td>
</tr>
<tr>
<td>Executable Path</td>
<td>Shows the actual path name of the executed command to start this process.</td>
</tr>
<tr>
<td>Total Memory</td>
<td>Shows the total memory allocated to this process.</td>
</tr>
<tr>
<td>Code Size</td>
<td>Shows the total memory allocated for code to this process.</td>
</tr>
</tbody>
</table>
8.13 Troubleshooting a Suspect or Bad Health Status

When the health status of an item changes from good to a suspect or bad state, you can look at the specific item and check the online help for suggested remedies.

1. In Novell Remote Manager, access Server Health Values or Server Health Services.
2. Look for the specific health item that has changed status.
3. View the information for the item that has changed by clicking the Info icon for the item.
   This information outlines the specific health criteria (thresholds) for green, yellow, or red statuses in that component. It also provides suggestions in some cases for what might be going wrong in that component if a yellow or red indicator is displayed.
4. Perform the recommended or appropriate action for the health item that has changed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Size</td>
<td>Shows the total memory allocated for data to this process.</td>
</tr>
<tr>
<td>Library Memory</td>
<td>Shows the total memory allocated for libraries to this process.</td>
</tr>
<tr>
<td>Dirty Pages</td>
<td>Shows the total memory that is dirty that belongs to this process.</td>
</tr>
<tr>
<td>Resident Pages</td>
<td>Shows the amount of memory that this process is using that has not been swapped out.</td>
</tr>
<tr>
<td>Tasks</td>
<td>Shows a list of tasks or threads belonging to this process.</td>
</tr>
<tr>
<td>File Descriptors</td>
<td>Shows a list of file descriptors that the process has open.</td>
</tr>
</tbody>
</table>
The Home icon and View File System section in Novell Remote Manager for Linux include the following links to these pages:

<table>
<thead>
<tr>
<th>Link</th>
<th>Page Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home icon</td>
<td>File System Management</td>
</tr>
<tr>
<td>View File System Listing</td>
<td>Directory Listing of / (root) directory</td>
</tr>
<tr>
<td>View Partition Information</td>
<td>Partition Information</td>
</tr>
</tbody>
</table>

From these pages you can perform the following tasks:

- Section 9.1, “Viewing Mounted Devices and Performing Actions on Them,” on page 64
- Section 9.3, “Viewing Partition Information,” on page 70
9.1 Viewing Mounted Devices and Performing Actions on Them

The File System Management page is the home page for Novell Remote Manager.

Figure 9-1  File System Management Page with Information Pages

You can access this page by clicking the Home icon (File System) link in the header frame.
The File System Management page provides a list of the server’s mounted devices. The devices that are shown are from the Linux mountable file, which is a list of other file systems mounted on this host’s file system.

You can view the percent of free space available on all mounted physical devices or external file systems that have actual disk space. Available disk space on virtual file systems is not shown. For information about how NSS reports space usage for volumes, see “Guidelines for Sizing Volumes” in the OES 2015 SP1: NSS File System Administration Guide for Linux.

To view specific information about each mounted physical device or external file system that has actual disk space, click the Information icon on the left. Clicking the Information icon displays one of the following types of pages:

- **File System Information.** This page shows the mount point, the file system type, the size of the mount point and the space in use. Clicking the Unmount button on this page, dismounts the remote file system shown. The Unmount button is available only on remotely mounted file systems such as NFS, NCP, and Samba.
- **NCP Share Information.** This page shows the volumes underlying file system type, mount point and status, and cache information.

You can browse any of these file systems by clicking the link in the Mount Location column. At this point, you can perform any of the tasks listed for browsing the servers file system. See “Browsing File Systems and Performing Actions on Them” on page 65.

### 9.2 Browsing File Systems and Performing Actions on Them

On the Directory List page, you can view the Linux POSIX file system and NSS file system from mount points or local partitions; browse directories and files; view and change attributes, directories, and files; and edit, delete, or rename files.

To access this page, click View File System > View File System Listing in the navigation frame.
The following table describes the actions necessary to access directories, files, and file and directory attributes from the Directory List page.

**Table 9-2  Directory List Page Tasks and Procedures**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse to a mount point, volume, directory, or local partition</td>
<td>Click the link for the mount point, volume, directory, or local partition under the Name column.</td>
</tr>
<tr>
<td>Move down the directory tree</td>
<td>Click the directory_name link.</td>
</tr>
<tr>
<td>Move up the directory tree</td>
<td>Click the double_dots (..) link.</td>
</tr>
<tr>
<td>Re-sort the list by name, size, or date and time.</td>
<td>Click the column heading that has a Sort icon next to it. The default sort for this listing is by the directory or file name.</td>
</tr>
<tr>
<td>View or change the attributes of a directory</td>
<td>Click the Attributes link. For information, see Section 9.2.1, “Viewing or Changing File or Directory Attributes,” on page 67.</td>
</tr>
<tr>
<td>View the size of a directory or file.</td>
<td>The Size column for a directory lists the size of all files and subdirectories in that directory.</td>
</tr>
</tbody>
</table>

From the Directory Listing page, you can perform the following tasks.

- Section 9.2.1, “Viewing or Changing File or Directory Attributes,” on page 67
- Section 9.2.2, “Viewing Details about Directories and Performing Actions on Them,” on page 67
9.2.1 Viewing or Changing File or Directory Attributes

Clicking the Attributes link opens the Directory Information page where you can view or change the attributes of the directory. For more information, see “Viewing Details about Directories and Performing Actions on Them” on page 67 and “Viewing the Details of a File and Performing Specific Actions” on page 69.

**IMPORTANT:** To set directory and file attributes for files on the NSS file system, go to Manage NCP Services > Manage Shares, the browse to locate the file and set its attributes. You can also use Novell iManager, the Novell Client, or Novell NetStorage.

Viewing attributes on NSS volumes, directories, and files conveys the status of the NSS file system directory and file attributes: Hidden (H), Read Only (Ro), Read/Write (Rw), and Execute (X). You can view these settings in Novell Remote Manager for Linux as a combination of Read, Write, and Execute fields for the User, Group, and Other categories. Although it appears that you can control these attributes using the selections on the Directory Information page, the selections do not actually control the conventional POSIX settings for NSS directories and files. For more information, see “Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions” in the OES 2015 SP1: File Systems Management Guide.

9.2.2 Viewing Details about Directories and Performing Actions on Them

1. Click the View File System > View File System Listing link in the navigation frame or click a Mount_Location_name link on the Home page.
2. On the Directory list page, browse to the directory you want to search in by clicking the directory_name link.
3. From the directory listing, click the Folder Information icon to the left of the directory or subdirectory you want to view information about or change the attributes of.
4. On the Directory Information page that is displayed, view the information or select/deselect the check box for the attributes that you want to change.
5. Click OK.
6. When viewing the details of a directory from the Directory Information page, you can also perform the following tasks for the selected directory:
   - Delete the directory and its contents
   - Rename the directory
   - Create a subdirectory in the directory
   - Create a symbolic link in the directory
9.2.3 Uploading a File to the Server

If you have rights to write to the current directory that you are viewing via Novell Remote Manager, you can use the Upload link to copy a file from your local machine or any other network directory to the currently selected directory.

You can upload only one file at a time. The file’s date and time are changed when performing this task.

To perform this task:

1. Click the View File System > View File System Listing link in the navigation frame or click a Mount_Location_name link on the Home page.
2. On the Directory list page, browse to the directory you want to upload a file to by clicking the directory_name link.
3. In the directory listing, click the Upload link at the top of the Directory listing page.
4. Browse to and select the file that you want to upload.
5. Click Upload.

9.2.4 Downloading a File from the Server to a Local Workstation

When you are browsing the server’s file system via Novell Remote Manager, you can download any file to your local machine by clicking the file name, and then saving the file to your local workstation.

1. Click the View File System > View File System Listing link in the navigation frame, or click a Mount_Location_name link on the Home page.
2. On the Directory/File List page, browse to or search for the file that you want to download.
3. Click the file_name link.
4. When prompted, save the target file to the desired location.
   - If the file opens rather than prompting you to save it, you can use the browser features to save the file.
### 9.2.5 Searching for Text in Files

On the Directory Listing page, you can do a GREP-type search (it accepts GREP wildcard characters) through the files in the current directory as well as subdirectories to find text in a file.

1. Click the View File System > View File System Listing link in the navigation frame or click a Mount Location name link on the Home page.
2. On the Directory list page, browse to the directory you want to search in by clicking the directory name link.
3. Click the Text Search link.
4. Specify the content, file name, or extension you want to search for and select whether you want to match the case.
5. (Optional) If you want to search all subdirectories as well, select Search Subdirectories.
6. Click Search.

   - If nothing is found, no files are listed under the search instructions.
   - If the search instructions are not valid, the page showing the directory you wanted to search is returned.
   - If the search instructions are valid, the results are displayed on a page with the search instructions.

   In the display results, you can
   - Click the file name link to view or download the file.
   - Click the File Information icon to view information about the file; change the attributes to it; or edit (conditional), rename, or delete the file.

   If the file is a simple text file or a file with an extension listed in the /opt/novell/nrm/nrmedit.txt file, you can also edit the file by clicking the Edit File button.

### 9.2.6 Viewing the Details of a File and Performing Specific Actions

1. Click the View File System Listing link in the navigation frame or click a Mount Location name link on the Home page.
2. On the Directory list page, browse the directories to the file, then click the File icon to the left of the file name.
3. On the File Information page that is displayed, view the information or specify the information required for the applicable task, and then click the applicable button for the task you want to perform.

   - For Attributes management, click the attributes that you want to select/deselect and then click OK.
   - For file management, use the Edit, Delete, or Rename buttons. The Edit button is available only on simple text files or files with the extensions listed in the /opt/novell/nrm/nrmedit.txt file.
If you want to save the file with an ANSI or UTF-8 encoding, select the appropriate option and click OK.

9.2.7 Viewing Individual Files

If your browser is set up to recognize a certain file extension (for example, .txt), you can browse to and click a file of that type to view it directly in Novell Remote Manager. Otherwise, you can download any file to your local machine by clicking the file name, and then saving it to a local workstation and opening it there. See Section 9.2.4, “Downloading a File from the Server to a Local Workstation,” on page 68.

9.3 Viewing Partition Information

If you need to get information about how a partition is laid out, you can get this information from the Partition Information page. This page shows you the major and minor numbers of the partition, the number of blocks in the partition, and its name.

To view partition information, click View Partition Information in the navigation frame.

Figure 9-3 Example Partition Information Page

<table>
<thead>
<tr>
<th>Partition Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>major</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>
The Manage Linux section in Novell Remote Manager (NRM) for Linux includes the following links to these pages from which you can perform the following tasks:

<table>
<thead>
<tr>
<th>Table 10-1 Manage Linux Section Tasks, Links, and Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
</tr>
<tr>
<td>Access VNC Console screens</td>
</tr>
<tr>
<td>View Kernel Modules Information</td>
</tr>
<tr>
<td>Shut down and restart the host</td>
</tr>
<tr>
<td>Manage packages</td>
</tr>
<tr>
<td>Manage processes</td>
</tr>
<tr>
<td>Schedule cron jobs to run</td>
</tr>
</tbody>
</table>

10.1 Accessing VNC Consoles

If VNC services are configured on the server, you can access the VNC consoles screens in Novell Remote Manager. The accessibility to the VNC consoles via Novell Remote Manager for Linux is limited to user *root*; it is not available to user Admin. This form of remote administration is less secure than SSH; therefore, we recommend using this feature only in a secure environment (behind a firewall).

**IMPORTANT:** VNC access is disabled by default to prevent cross-site scripting. You must disable the HttpOnly setting in the `/etc/opt/novell/httpstkd.conf` file in order to enable the VNC console display. For information, see Section A.5, “HttpOnly Command,” on page 158.

1 If VNC services are not configured on the server, you can configure them as follows:

1a In YaST, log in as the *root* user, then click Network Services > Remote Administration.

1b On the Remote Administration page, select the following options:

- Allow Remote Administration
- Open Port in Firewall (default port is 5801)

1c Click Finish.
1. Restart the display manager by entering the following command at the command line:
   
   `rcxdm restart`

2. Verify that pop-up blocking is disabled in your web browser.

3. Log in to Novell Remote Manager as the root user.

4. Select Manage Linux > VNC Consoles.

5. If VNC Consoles is disabled, a message is displayed instead of the console. You must disable the HttpOnly setting in the `/etc/opt/novell/httpstkd.conf` file in order to enable the VNC console display. For information, see Section A.5, “HttpOnly Command,” on page 158.

6. Click the 1024 X 728 button on the VNC Console Screens page.

   Clicking the VNC Consoles link opens a Java applet in a secondary browser window. The following table explains what you can do from this window.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use any of the screens listed as though you were at the server console.</td>
<td>Use the keyboard or mouse as though you were at the server console.</td>
</tr>
<tr>
<td>Disconnect from the console.</td>
<td>Click the Disconnect button on this page.</td>
</tr>
<tr>
<td>Change any of the VNC client options currently selected.</td>
<td>Click the Options button.</td>
</tr>
<tr>
<td>Access the VNC client clipboard and cut or paste any commands that you might want to execute in an active terminal shell.</td>
<td>Click the Clipboard button.</td>
</tr>
<tr>
<td>Restart the server.</td>
<td>Click the Send Ctrl+Alt+Del button.</td>
</tr>
<tr>
<td>Refresh the current screen you are viewing.</td>
<td>Click the Refresh button.</td>
</tr>
</tbody>
</table>

**Figure 10-1** illustrates a user accessing YaST on a remote server from the user’s desktop browser. To access YaST on the remote server, the user did the following:

1. Clicked the VNC Consoles link in the navigation frame.
2. Clicked the 1024 X 728 button on the VNC Consoles Screens page.
3 Logged into Linux.

4 Clicked **Computer > System > YaST**.

*Figure 10-1* Example Access of YaST through NRM VNC Console Screens Linux on a GNOME Desktop.

## 10.2 Viewing Kernel Modules

Clicking the **View Kernel Modules** link in the navigation frame displays the Kernel Module Listing page. On this page you can view the status of the modules that have been compiled into the Linux kernel on this system. Printing this page can be useful to document your system as you make changes or upgrades to it in the future.

The information shown on this page is equivalent to the information in the `lsmod` shell command plus the Live information or equivalent to viewing the `proc\modules` file.
10.3 Shutting Down and Restarting the Host

Clicking the Down/Restart link in the navigation frame displays the Down/Reset Options page. You can use these options to shut down or reset the host.

The following table describes the specific actions of each option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down</td>
<td>Forces the host to shut down immediately.</td>
</tr>
<tr>
<td>Reset</td>
<td>Forces the host to shut down immediately, then warm boots the computer.</td>
</tr>
</tbody>
</table>

Using either of the options additionally forces the host to perform the following actions:

- Update the cache buffers to disks
- Close all open files

**WARNING:** If files are open and changes have not been saved to the host, some data loss might occur. Users might need to save changes locally until the host is started again.

If the application that is being used to access the file creates a temporary file and locks the file, you might also need to search for and remove the temporary file.
For example, Microsoft Word creates a system file that begins with ~$, such as ~$myfile8.doc. OpenOffice and LibreOffice create a hidden file that begins with .~lock, such as .~lock.myfile10.odt. You can view the temporary files by selecting Manage Shares, then navigating the NCP volume or NSS volume to the folder where the open file is stored.

- Update the appropriate file system tables
- Exit the host from the network
- Unmount all file systems

## 10.4 Managing Packages

Clicking the View Package Information link displays the Packing Information page. On this page you can view the following information about each package that is installed on the system:

- Name
- Group
- Version
- Release
- Vendor

![Figure 10-3 Example Package Information Page](image)

On the View Package Information page and subsequent pages, you can perform these tasks using the following procedures:
Table 10-4  View Package Information Page Tasks and Procedures

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort the listed packages by name, group,</td>
<td>Click the Sort icon ▼ at the top of the applicable column.  The default sort is by name.</td>
</tr>
<tr>
<td>or vendor</td>
<td></td>
</tr>
<tr>
<td>View more detailed information about an</td>
<td>Click the link for the applicable package under the Name column.</td>
</tr>
<tr>
<td>installed package</td>
<td></td>
</tr>
</tbody>
</table>
| Remove an installed package                | 1. Click the link for the package under the Name column.  
                                            | 2. Click Remove.                                                                                  |
| Install a new package that you have        | 1. Click Install.  
                                            | 2. Browse to the location where you uploaded the package to.  The browse starts at the root of   |
| downloaded to the host                     | 3. Click Install.  
                                            | the host.                                                                                       |
|                                           | The selected package’s file path is transferred to the RPM File Path field on the Package     |
|                                           | Installation page.                                                                            |
|                                           | When the Install button is clicked on the View Package Information page, Novell Remote       |
|                                           | Manager attempts to install the specified RPM file using the Linux RPM utility.                |

The following figure shows a sample of the details you see when you click the package_name link.  

Figure 10-4  Detailed Information Page for the 3ddiag Example Package

3ddiag

<table>
<thead>
<tr>
<th>Name</th>
<th>3ddiag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>0.7.42</td>
</tr>
<tr>
<td>Vendor</td>
<td>SUSE LINUX Products GmbH, Nuernberg, Germany</td>
</tr>
<tr>
<td>Release</td>
<td>32.25</td>
</tr>
<tr>
<td>Install Date</td>
<td>Thu Jun 16 11:11:19 2016</td>
</tr>
<tr>
<td>Build Host</td>
<td>baur</td>
</tr>
<tr>
<td>Group</td>
<td>System/Base</td>
</tr>
<tr>
<td>Source RPM</td>
<td>3ddiag-0.7.42-32.25.src.rpm</td>
</tr>
<tr>
<td>Size</td>
<td>53177</td>
</tr>
<tr>
<td>License</td>
<td>GPL V2 or later</td>
</tr>
<tr>
<td>Signature</td>
<td>RSA/8, Tue Feb 24 01:23:20 2009, Key ID 03a5c3693079ed54</td>
</tr>
<tr>
<td>Package</td>
<td><a href="http://bugs.opensuse.org">http://bugs.opensuse.org</a></td>
</tr>
<tr>
<td>Summary</td>
<td>A Tool to Verify the 3D</td>
</tr>
<tr>
<td>Description</td>
<td>Configuration.</td>
</tr>
<tr>
<td>Authors</td>
<td>Stefan Dirsch</td>
</tr>
<tr>
<td>Distribution</td>
<td>SUSE Linux Enterprise 11</td>
</tr>
</tbody>
</table>

10.5  Managing Processes

Clicking the View Process Information link in the navigation frame displays the Process Information page. On this page, you can view a list of all the processes as well as their state in the host and perform the actions listed in the following table.
Table 10-5  Process Information Page Tasks and Procedures

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort the process by name (in alphabetical order by default), by process ID, by CPU Usage, or by Memory Usage</td>
<td>Click the Sort icon ▼ at the top of the applicable column.</td>
</tr>
<tr>
<td>View more specific information about a listed process</td>
<td>Click the link for the applicable process under the Name column.</td>
</tr>
<tr>
<td>Kill a process</td>
<td>1. Click the link for the applicable process under the Name column.</td>
</tr>
<tr>
<td></td>
<td>2. Click Kill.</td>
</tr>
</tbody>
</table>

The process information is obtained from the `stat` file that is available for each process ID in the `/proc` directory. Process information can also be retrieved at the command line by using the Linux `top` command.

Table 10-6 on page 77 describes the parameters reported for each process.

Table 10-6  Process Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The process name.</td>
</tr>
<tr>
<td>Owner</td>
<td>The process owner; the user who started the process.</td>
</tr>
<tr>
<td>ID (Status)</td>
<td>The process ID of the task, and the current state of the task. The states are Sleep (S), Running (R), Traced (T), or Zombied (Z). These states are modified by a trailing &lt; for a process with a negative nice value, N for a process with positive nice value, and W for a swapped-out process (this does not work correctly for kernel processes).</td>
</tr>
<tr>
<td>CPU Usage %</td>
<td>The task's share of the CPU time since the last screen update, expressed as a percentage of total CPU time per processor.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the task.</td>
</tr>
<tr>
<td>Run Time</td>
<td>The total CPU time the task has used since it started.</td>
</tr>
<tr>
<td>Physical Memory</td>
<td>The physical memory value is the amount of physical memory in bytes that the task is using. The value in parentheses (%) is the percentage of RAM memory that this represents. The Linux <code>top</code> command reports this information in kilobytes.</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>The virtual memory is the amount of memory in bytes that the task is using to hold the code, data, and stack space memory. The Linux <code>top</code> command reports this information in kilobytes. Virtual Memory is the value reported by the <code>RSS</code> switch for the <code>top</code> command.</td>
</tr>
</tbody>
</table>
10.6 Scheduling cron Jobs to Run on the Server

Rather than entering commands on the command line to run a cron job at a specific time, you can use a form on the Schedule Task page to schedule cron jobs—that is, to execute commands or scripts (groups of commands) automatically at a specified time/date—that you want to run at this server. Any cron job is valid.

Scheduling a task creates a cron job and stores it in the /etc/cron.d directory. The command is specified to run with the name of whatever user name you are logged in with when you add the command. The user name must have the necessary permissions to perform the command you add.

**IMPORTANT:** When you set up cron commands, you must log into Novell Remote Manager as the root user.

If no mail service is configured, you might find the output of your commands in the local mailbox directory as a plain text file. By default, this is /var/spool/mail/root.
To create a new scheduled command:

1. Complete the required information on the Schedule Task page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Information to Provide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a brief description of the command you want to run.</td>
</tr>
<tr>
<td></td>
<td>64 character limit</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Send message to log out daily at 10 p.m.</td>
</tr>
<tr>
<td></td>
<td>This description is displayed as the name of the scheduled job in the Currently Scheduled CRON Jobs list.</td>
</tr>
<tr>
<td>Command to Execute</td>
<td>Type the command exactly as you would at a command line.</td>
</tr>
<tr>
<td></td>
<td>All cron job entry types are valid except for lists and step values.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Type the time you want the command to run.</td>
</tr>
<tr>
<td>Start Day</td>
<td>If you want to run the command once a week, specify the day of the week, then place an asterisk * in the Month and Day fields.</td>
</tr>
<tr>
<td></td>
<td>If you want to run the command only once or monthly, specify a Month and Day setting, then place an asterisk * in the Day of the Week field.</td>
</tr>
<tr>
<td></td>
<td>If you want to run the command monthly, specify a Day setting, then place an asterisk * in the Start Day and Month fields.</td>
</tr>
<tr>
<td></td>
<td>If you do not want to specify a value for a field, place an asterisk * in the field.</td>
</tr>
</tbody>
</table>

2. Click Submit.

After you schedule a job, it is displayed at the top of the page under the Currently Scheduled CRON Jobs heading. Jobs that you create manually also display in the list.
To change the schedule of a job that you have already scheduled:

1. Click the link for the job you want to change.
2. Change the schedule.
3. Click Submit.

To delete the schedule of a job that you have already scheduled:

1. Click the link for the job you want to delete.
2. Click Delete.

To return the settings in the fields to the default settings of the current day and time, click Reset.
Managing Hardware

The Manage Hardware section in Novell Remote Manager (NRM) for Linux includes the following links to pages from which you can perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Link</th>
<th>Page Displayed</th>
<th>For More Info, See</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Processor information</td>
<td>View Processors</td>
<td>Processor Information</td>
<td>&quot;Viewing Processors&quot; on page 81</td>
</tr>
<tr>
<td>View Interrupt information</td>
<td>Interrupt Information</td>
<td>Interrupts</td>
<td>&quot;Viewing Interrupt Information&quot; on page 82</td>
</tr>
<tr>
<td>View memory I/O information</td>
<td>IO Memory Information</td>
<td>I/O Memory Information</td>
<td>&quot;Viewing I/O Memory Information&quot; on page 83</td>
</tr>
<tr>
<td>View port I/O information</td>
<td>IO Port Information</td>
<td>IO Port Information</td>
<td>&quot;Viewing I/O Port Information&quot; on page 84</td>
</tr>
<tr>
<td>View SMBIOS information</td>
<td>SMBIOS Information</td>
<td>SMBIOS Information</td>
<td>&quot;Viewing SMBIOS Information&quot; on page 85</td>
</tr>
</tbody>
</table>

### 11.1 Viewing Processors

Clicking the View Processors link under the Manage Hardware heading in the navigation frame displays the Processor Information page. On this page you can view information about each processor on this host.

Information about the processor speed as well as the local cache sizes is useful in determining how much work a processor can do.

This information is equivalent to the information you would see in the /proc/cpuinfo file.

**Figure 11-1 Example Processor Information Page**

In a virtualized environment, the processor information is reported from the perspective of the server where you connected.

- **Host Server**: When you connect to Novell Remote Manager by using the host server IP address, the report contains information about all processors on the system.
**Guest Server:** When you connect to Novell Remote Manager by using the guest server IP address, the report contains information about the physical hardware in use, but only for the number of processors you assign to the virtual machine.

The guest server reports the same information about a processor as if it owned the actual hardware on the server. The Virtual Machine Monitor component of the virtualization software emulates a complete hardware environment in the virtual machine for the guest server. The guest server OS is unaware that it shares the hardware resources with other virtual machines and the host.

The actual usage statistics of the physical processors are not known by Novell Remote Manager. You could use the Virtual Machine Manager to see that type of information.

### 11.2 Viewing Interrupt Information

Clicking the **Interrupt Information** link under the **Manage Hardware** heading in the navigation frame displays the Interrupts page, which includes the following:

**Table 11-2  Interrupts Page**

<table>
<thead>
<tr>
<th>Category</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interrupt</td>
<td>Interrupt number or name of an interrupt that might be generated.</td>
</tr>
<tr>
<td>CPU <em>number</em></td>
<td>Number of interrupts that have occurred on a given processor.</td>
</tr>
<tr>
<td>Route-Trigger Method</td>
<td>How the interrupt is being delivered to the processor and the method of interrupting the processor.</td>
</tr>
<tr>
<td>Device</td>
<td>Name of the device driver that is generating the interrupt.</td>
</tr>
</tbody>
</table>
11.3 Viewing I/O Memory Information

Clicking the IO Memory Information link under the Manage Hardware heading in the navigation frame displays the I/O Memory Information page, which includes the following:

**Table 11-3  I/O Memory Information Page**

<table>
<thead>
<tr>
<th>Category</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Address</td>
<td>I/O memory range that a given device is using.</td>
</tr>
<tr>
<td>Device Description</td>
<td>A description of the device that is using a given I/O memory range.</td>
</tr>
</tbody>
</table>
### 11.4 Viewing I/O Port Information

Clicking the **IO Port Information** link under the **Manage Hardware** heading in the navigation frame displays the I/O Port Information page, which includes the following:

<table>
<thead>
<tr>
<th>Category</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>IO Address</td>
<td>Shows the I/O port range that a given device is using.</td>
</tr>
<tr>
<td>Device Description</td>
<td>Shows the name of the device that is using a given I/O port range.</td>
</tr>
</tbody>
</table>
11.5 Viewing SMBIOS Information

Clicking the SMBIOS Information link under the Manage Hardware heading in the navigation frame displays the SMBIOS Information page. On this page, you can view details about the BIOS hardware in each host without physically removing the hardware cover. You also have access to information that is available only through the management system.

Each link shows the type of device that is available in the BIOS of the host computer.

You might see information types such as the following. The types displayed vary depending on the hardware in your system.

- BIOS
- System
- Base Board
- System Enclosure or Chassis
- Processor
- Cache
- Port Connector
- System Slots
- On Board Device
- OEM Strings
- BIOS Language
- System Event Log
- Physical Memory Array
- Memory Device
- Memory Array Mapped Address
- Memory Device Mapped Address
- Hardware Security
- System Boot

Selecting an information type displays information contained within SMBIOS for the type selected. For example, to see all the BIOS information, click the **BIOS Information** link. See Figure 11-5.

*Figure 11-5  Example SMBIOS and BIOS Information Pages*
12 Using Group Operations

The Use Group Operations section in Novell Remote Manager (NRM) for Linux includes the following links to pages from which you can perform the following tasks:

Table 12-1 Use Group Operations Tasks, Links, and Pages

<table>
<thead>
<tr>
<th>Task</th>
<th>Link</th>
<th>Page Displayed</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access an existing group</td>
<td>Select Group</td>
<td>Select Group</td>
<td>&quot;Accessing an Existing Group&quot; on page 93</td>
</tr>
<tr>
<td>Build and configure a new monitoring group</td>
<td>Configure New Group</td>
<td>Group Monitoring Operations</td>
<td>&quot;Building and Configuring a Monitoring Group&quot; on page 88</td>
</tr>
<tr>
<td>Change an existing group</td>
<td>Select Group</td>
<td>Select Group</td>
<td>&quot;Changing an Existing Group&quot; on page 93</td>
</tr>
<tr>
<td>Define or edit Group Monitoring types</td>
<td>NRM Health Types</td>
<td>Novell Remote Manager Health Monitoring Engine (NRM Health Types)</td>
<td>&quot;Defining or Editing Group Monitoring Types&quot; on page 96</td>
</tr>
<tr>
<td>Delete an existing group</td>
<td>Select Group</td>
<td>Select Group</td>
<td>&quot;Deleting an Existing Group&quot; on page 94</td>
</tr>
<tr>
<td>Scan the network for items to monitor on the network.</td>
<td>Configure New Group &gt; right-click &gt; click Network Discovery</td>
<td>Network Discovery</td>
<td>&quot;Discovering Items on the Network to Monitor&quot; on page 97</td>
</tr>
<tr>
<td>Generate and view server reports</td>
<td>Configure New Group &gt; right-click &gt; click Save Group</td>
<td>Group Monitoring Operations</td>
<td>&quot;Generating and Viewing Server Reports&quot; on page 94</td>
</tr>
<tr>
<td>Save a new group</td>
<td>Configure New Group &gt; right-click &gt; click Save Group</td>
<td>Save Group</td>
<td>&quot;Saving a Group&quot; on page 92</td>
</tr>
<tr>
<td>View group operations monitored items</td>
<td>View Monitored Items</td>
<td>Novell Remote Manager Health Monitoring Engine - Monitored Items</td>
<td>&quot;Viewing Monitored Items&quot; on page 95</td>
</tr>
<tr>
<td>View group operations defined NRM health types</td>
<td>NRM Health Types</td>
<td>Novell Remote Manager Health Monitoring Engine - NRM Health Types</td>
<td>&quot;Viewing Group Monitoring Types&quot; on page 95</td>
</tr>
</tbody>
</table>

Using the group features involves performing one or more of the following tasks:

2. (Optional) Saving a Group (page 92).
   You only need to perform this step if you want to use the group at a later time.
The monitoring operations start immediately. Other tasks, such as running reports require additional steps.

4. (Conditional) Accessing an Existing Group (page 93).

### 12.1 Building and Configuring a Monitoring Group

Novell Remote Manager lets you build and configure groups of items for monitoring Linux server or NetWare server health, as well as providing various statistics for servers running other operating systems. A few of the preconfigured monitoring item types are NRM Health Status for a single server or a group of servers, Ping to a specific port, IP connectivity, LDAP Directory Root Search, and status of connectivity to a web page.

Monitoring items can be defined and represented by an icons on a page as shown in the following figure. The icons can represent a single item or a group of items.

*Figure 12-1  NRM Server Health Example Group*

To build and configure a new monitor group:

1. Click the **Configure New Group** link in the navigation frame.
2. Right-click the Group Monitoring Operations page.

**TIP:** If your browser does not support right-click functionality, try double-clicking the Reports icon in the upper right corner of the page.
You should see a pop-up similar to the following:

Add Item
Configure New Group
Full Screen
Group Configuration
Network Discovery
Refresh
Save Group
Select Group
Show Hidden Items
NRM Reports & Operations

The menu options are:
- Add Item
- Configure New Group
- Full Screen
- Group Configuration
- Network Discovery
- Refresh
- Save Group
- Select Group
- Show Hidden Items
- NRM Reports & Operations

3 Click Add Item, and do the following:

3a Complete the Monitoring Item Configuration form.
For each item you add to a group or want to change from the default setting (health monitor), complete the following options on the Monitoring Item Configuration form.

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Type</td>
<td>Specify one of the following types:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Label</strong>: Text information to use as a label on the group monitor display. Lets you identify each group specifically as needed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>LDAP Directory Root Search</strong>: Shows the response when trying to ping port 389 of the specified LDAP server. Credentials are not used. This is useful to monitor the status of your LDAP servers in your network.</td>
</tr>
<tr>
<td></td>
<td>- <strong>NRM Group</strong>: Shows the health status of a group of servers. Lets you access the specific health page for each server in the group.</td>
</tr>
<tr>
<td></td>
<td>- <strong>NRM Health Monitor</strong>: Shows the health status of each server in the group. Lets you access the specific health page for each server in the group.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Ping (ICMP)</strong>: Shows the response when sending ping requests to the specified DNS name or IP address.</td>
</tr>
<tr>
<td></td>
<td>- <strong>TCP/IP Port Query</strong>: Shows response activity of a designated TCP/IP service. This query attempts to make a TCP connection to the specified address and port. Returns green (good) health if any services is listening. For example, you could set up a health monitoring item to tell you whether your GroupWise server is still listening for logins from clients. The only states that are returned are green (good), which means the connection was successful, and red (bad), which means the connection was not successful.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Web page</strong>: Shows the response when trying to determine if the communication is working to a server that hosts a website. It does not monitor specific websites on the server. It does not monitor whether the web service is running. Specify only the portion of the web address (URL) that a DNS server can resolve to an IP address; do not include a subdirectory. For example, specify <a href="http://www.novell.com">www.novell.com</a>, but not <a href="http://www.novell.com/support">www.novell.com/support</a>. If you specify a subdirectory, the DNS name cannot be resolved, and a Can't Connect health status is reported.</td>
</tr>
<tr>
<td>Name</td>
<td>Provide a descriptive name for the item.</td>
</tr>
<tr>
<td>Item Address/URL</td>
<td>Specify the IP address for the server that you want to monitor or ping, or specify the DNS name of the server that hosts the web page. The address can be an IP address or DNS name. Do not specify the HTTP:// portion of a URL.</td>
</tr>
<tr>
<td>Port</td>
<td>The default is provided. You can type a different port to use.</td>
</tr>
<tr>
<td>Use Single Sign on NRM Credentials</td>
<td>When selected (default), the credentials used to access this items’ data are the same as the credentials that the user logged into Novell Remote Manager with.</td>
</tr>
<tr>
<td></td>
<td>When deselected, enter the credential necessary to access the item in the User Name and Password fields.</td>
</tr>
<tr>
<td>Hide Normal Status</td>
<td>When selected, only items that are in an abnormal state are displayed.</td>
</tr>
<tr>
<td></td>
<td>If you want to monitor all statuses, leave the check box deselected.</td>
</tr>
</tbody>
</table>
Using Group Operations

You can also define your own monitoring types or edit the default defined health types by editing the XML data in /opt/novell/nrm/NRMGroupHealthInfo file. For more information, see "Defining or Editing Group Monitoring Types" on page 96.

3b Click Add.
3c Drag the monitor items to the desired location.
3d Repeat Step 3a through Step 3c for each item that you add.

4 (Optional) If you want to change any of the following, change the configuration of the group:

- The label for the group
- The graphic displayed
- The refresh rate
- The suspect and critical email notification for the group

4a Right-click the customized Group page, then click Group Configuration.
4b Complete the fields as desired on the Group Operations Configuration form.

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Color</td>
<td>Black is the default. You can select any other color from the drop-down list.</td>
</tr>
<tr>
<td>Text Background Color</td>
<td>Clear is the default. You can select any other color in the drop-down list.</td>
</tr>
</tbody>
</table>

You can also define your own monitoring types or edit the default defined health types by editing the XML data in /opt/novell/nrm/NRMGroupHealthInfo file. For more information, see "Defining or Editing Group Monitoring Types" on page 96.

3b Click Add.
3c Drag the monitor items to the desired location.
3d Repeat Step 3a through Step 3c for each item that you add.

4 (Optional) If you want to change any of the following, change the configuration of the group:

- The label for the group
- The graphic displayed
- The refresh rate
- The suspect and critical email notification for the group

4a Right-click the customized Group page, then click Group Configuration.
4b Complete the fields as desired on the Group Operations Configuration form.

Group Operations Configuration

<table>
<thead>
<tr>
<th>Display Options</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Page Title</td>
<td></td>
</tr>
<tr>
<td>Background Graphic</td>
<td>NRMDefaultGroupMac.JPG</td>
</tr>
<tr>
<td>Refresh Rate</td>
<td>30 Seconds</td>
</tr>
<tr>
<td></td>
<td>Click Apply</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>The display options let you control the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Monitor Page Title</strong>: Specify a title to be shown at the top of the monitor page in the header area when the page is built.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Refresh Rate</strong>: Specify the number of seconds between status queries to the server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Background Graphic</strong>: Select a graphic from the drop-down list for the monitor items to be displayed on. This option can be helpful if you want to show specific locations of the item being monitored.</td>
</tr>
<tr>
<td></td>
<td>If you want to add a customized graphic, add it to the /opt/novell/nrm/NRMGroupMaps directory.</td>
</tr>
</tbody>
</table>

4c Click Apply.

5 Perform the desired task, or save the group and perform the task later.

In this release, the only task you can perform on Linux servers is to compare the server up times.
6 (Optional) If you want to reuse the group, save the group.

6a Right-click the *customized Group page*, then click *Save Group*.

We recommend using a name that represents the group you built.

6b (Conditional) If you haven’t saved any groups, you might need to extend the schema for NRM group operations before you can save the group.

Extending the schema is required only once per eDirectory tree. If the host is connected to a pre-existing NetWare 6.5 or later network, then extending the schema is not necessary.

6c Click *Save Group* and perform the required steps to save the group to a local server or save it and associate it with an eDirectory object.

See “Saving a Group” on page 92.

12.2 Saving a Group

You can save the configuration of the group so you can access this page again without completing the configuration options. You can save a group to the local server or associate with an eDirectory object and save it.

12.2.1 Saving the Group to the Local Server

1 While viewing the group you just created or edited, right-click the *customized Group page*, then click *Save Group*.

2 In the *Group Name* field, specify a name for the group or select a group name that you want to replace from the group list.

We recommend using a name that represents the group you built.

3 Click *Save Group*.

This saves the group to a file with that name in the */opt/novell/nrm/NRMGroups* directory.

12.2.2 Saving the Group and Associating It with an eDirectory Object

You can save a group and associate it with a User or Group eDirectory object. This is helpful when you want to access the configuration and you don’t want to save the configuration to a specific server (for example, if the server is down but you want it to be part of the operation or if you want to run the operation while one of the servers is not functioning properly).

Only one group can be associated to an object.

1 While viewing the group you just created or edited, right-click the *customized Group page*, then click *Save Group*.

2 In the *Make This the Group Monitor for This Object* field, specify a User or Group object that you want to associate this group with.

You can browse to the user or group by clicking the *Browse link* icon or by typing the full content name of the object.

3 Click *Save Group*.
12.3 Accessing an Existing Group

After a group has been saved to the server, you can access the group again to run reports or change the attributes of the group.

1. Click the Select Group link in the navigation frame.
2. On the Server Group page, select the desired group from the drop-down list.
3. Click Build Group.

12.4 Changing an Existing Group

After accessing an existing group (see “Accessing an Existing Group” on page 93), you might want to change it using one of the following procedures.

<table>
<thead>
<tr>
<th>Table 12-2 Changing an Existing Group Tasks and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want to</td>
</tr>
<tr>
<td>Change the configuration of an existing group.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>See the details of the server health or the monitoring type.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Edit an existing item in the group.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Delete a server or monitor item from a group.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Change the display to a full screen in your browser window.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
12.5 Deleting an Existing Group

To delete a group:

1. Click the Select Group link in the navigation frame.
2. On the Server Group page, select the desired group from the drop-down list.
3. Click Delete Group.

12.6 Generating and Viewing Server Reports

Running Server Comparison reports on a group of servers can help you determine which servers need to be updated or have configurations changed, why operations on that server might be sluggish, or which servers are receiving the most action.

In this release, you can run only one report, the “Compare Server Up Time Report” on page 94.

12.6.1 Compare Server Up Time Report

Run this report to see which servers might need replacing or tuning to keep them running longer. This report gives you an idea how long each server in the group has been running without being restarted.

1. Build the monitor group or select a group previously saved.
   See “Building and Configuring a Monitoring Group” on page 88 or “Accessing an Existing Group” on page 93.
2. Right-click the customized Group page.
3. Click NRM Reports & Operation.
4. Click Compare Server Up Times.
   A report similar to the following is returned.

<table>
<thead>
<tr>
<th>Server Up Time Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
</tr>
<tr>
<td>OES-Linux-s2</td>
</tr>
<tr>
<td>OES-Linux-s1</td>
</tr>
</tbody>
</table>

- Server has been up less than one hour.
- Server has been up less than one day.
12.7 Viewing Monitored Items

If you have several groups defined and you want to see which items are being monitored from this server without opening each group, click View Monitored Items.

This page lists all of the items currently being monitored by the Novell Remote Manager overall health monitoring engine on this server. For information about how this status is calculated for a server, see the following:

- For OES 2015 or later servers, see “Viewing the Overall Server Health Status” on page 40
- For OES 11 SP2 servers, see “Viewing the Overall Server Health Status” on page 40

If an item has not been monitored for more than 3 minutes, it is removed from the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Shows the overall health indicator icon for the item</td>
</tr>
<tr>
<td>Item Name</td>
<td>The name assigned to the item when it was defined in a Novell Remote Manager health monitoring group.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of item being monitored, such as NRM health, ping status, web page.</td>
</tr>
<tr>
<td>Address</td>
<td>The third column is the address that Novell Remote Manager uses to check the items health status.</td>
</tr>
<tr>
<td>Last Check Time</td>
<td>The last time that a Novell Remote Manager group requested the health status of this item.</td>
</tr>
<tr>
<td>Monitoring Start Time</td>
<td>The that health monitoring was started for this item.</td>
</tr>
</tbody>
</table>

If this server’s utilization is high due to the monitoring occurring on this server, you might consider moving some of the monitoring to another location.

12.8 Viewing Group Monitoring Types

Clicking the NRM Health Types link in the navigation frame displays the Novell Remote Manager Health Monitoring Engine - NRM Health Types content. This page gives you an overview of the Group Monitoring types that are defined on the current host. The legend shows the statuses you might see when you are monitoring groups of hosts with various monitored items and is a graphical view of the items defined in the /opt/novell/nrm/NRMDGroupHealthInfo file.
12.9 Defining or Editing Group Monitoring Types

If you want to add a Group Monitoring type to the group monitoring that is not defined or change the label of any of the predefined types, you can access the `/opt/novell/nrm/NRMGroupHealthInfo` file and make changes to it.

Each item is defined between the beginning and ending NRM_Health_Item_Definition XML tags as shown below.
12.10 Discovering Items on the Network to Monitor

If you want to scan the network for specific services, you can access the Network Discovery page and specify the host and ports that should be scanned for. After discovering the items on the network, you can click the item and add it to the current group for future monitoring.

Using this feature can help you to quickly gather the information you need to create monitoring groups.

To access this page, do the following:

1. In the navigation frame, click Use Group Operations > Configure New Group or Select Group.
2. Right-click the applicable group page displayed.
3. Verify that the browser you are using will accept pop-up dialog boxes.
4. Click Network Discovery.

The Network Discovery page is displayed:

<table>
<thead>
<tr>
<th>Network Scan Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Name/IP Address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Select a Network Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan available Hosts (ping/ICMP Echo)</td>
</tr>
<tr>
<td>Scan for Web Servers (port 80)</td>
</tr>
<tr>
<td>Scan for LDAP Servers (port 389)</td>
</tr>
<tr>
<td>Scan for Novell Remote Manager Servers (port 8008/8009)</td>
</tr>
<tr>
<td>Scan for Services (user supplied port)</td>
</tr>
</tbody>
</table>
To perform the scan, do the following:

1. Access the Network Discovery page.
2. Do the tasks specified in the following table:

   The **Network Scan Parameter** fields determine which hosts or ports should be scanned.

   The **DNS Name / IP Address** field is an IP address is used with the subnet mask to determine the range of IP addresses to be scanned. These fields default to the IP address of the current Novell Remote Manager host and a class C subnet mask. For example, if you wanted to scan for all the active hosts in the class B range of 137.65 subnet, you might set the IP address to 137.65.1.1 and the subnet mask to 255.255.0.0.

   Instead of scanning for all hosts that respond on the network, you can scan for hosts with specific services available.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **Scan the network for hosts that are responding to ICMP Echo Requests in the network within a specified subnet.** | 1. Accept the default IP address or DNS name and subnet mask information or change it.  
   2. Click **Subnet Scan**. |
| **Scan the network for hosts with port 80 open and listening for connections (Web Servers) within a specified subnet.** | 1. Accept the default IP address or DNS name and subnet mask information or change it.  
   2. Click **Web Server Scan**. |
| **Scan the network for hosts with port 389 open and listening for connections (LDAP Servers) within a specified subnet.** | 1. Accept the default IP address or DNS name and subnet mask information or change it.  
   2. Click **LDAP Server Scan**. |
| **Scan the network for hosts with port 8009 open and listening for connections (Hosts with Novell Remote Manager configured for the default ports) within a specified subnet.** | 1. Accept the default IP address or DNS name and subnet mask information or change it.  
   2. Click **NRM Agent Scan**. |
| **Scan the network for hosts with user_defined_port open and listening within a specified subnet.** | 1. Accept the default IP address or DNS name and subnet mask information or change it.  
   2. Click **Service Scan**. |

After scanning for a desired service, a Network Discovery page is displayed showing results for all hosts with the ports.

You can do the following task with the information returned:

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **See more information about the scanned host.** | 1. Click the **Web Service More Info** icon for the applicable host on the Network Discovery page.  
   2. View the information on the page that is returned. |
| **Add the host to the current group.** | 1. Click the **Add Item to Group** icon for the applicable host on the Network Discovery page.  
   2. Complete the required information on the Add New Monitor Item page, then click **Add**.  
   Most of the information is completed by default. |
Managing NCP Services

This section provides an overview of tasks that can be performed when the NCP Server and Dynamic Storage Technology plug-in is installed in Novell Remote Manager.

For information about using and managing NCP Server and NCP volumes on Open Enterprise Server (OES) 2015 SP1, see the *OES 2015 SP1: NCP Server for Linux Administration Guide*.

For information about using and managing NSS volumes on OES 2015 SP1, see the *OES 2015 SP1: NSS File System Administration Guide for Linux*.

The Manage NCP Services section in Novell Remote Manager for Linux includes the following links to these pages:

**Table 13-1  Links for Managing NCP Services**

<table>
<thead>
<tr>
<th>Link</th>
<th>Page Displayed</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Inventory Reports</td>
<td>NCP Inventory Reports</td>
<td>Section 13.3, &quot;Generating Inventories for Directories or NCP Volumes,&quot; on page 115</td>
</tr>
<tr>
<td></td>
<td>• Generate report</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Display last report</td>
<td></td>
</tr>
<tr>
<td>View Trustee Reports</td>
<td>NCP Trustee Reports</td>
<td>Section 13.6, &quot;Generating and Viewing NCP Trustee Reports for NSS Volumes,&quot; on page 123</td>
</tr>
<tr>
<td></td>
<td>• Generate report</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Display last report</td>
<td></td>
</tr>
<tr>
<td>Manage Shares</td>
<td>NCP Shares</td>
<td>&quot;Managing NCP Volumes&quot; in the <em>OES 2015 SP1: NCP Server for Linux Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td>• Active shares listing for NSS volumes and NCP volumes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Information about shares, including open files</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Create new share</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Delete existing share</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NCP/NSS bindings</td>
<td></td>
</tr>
<tr>
<td>Manage Server</td>
<td>NCP Manage Server</td>
<td>&quot;Managing NCP Server&quot; in the <em>OES 2015 SP1: NCP Server for Linux Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td>• Server parameters for NCP Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Global policy parameters for Dynamic Storage Technology</td>
<td></td>
</tr>
</tbody>
</table>
From these pages you can perform the following tasks:

- Section 13.1, “Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux,” on page 100
- Section 13.2, “Browsing NSS Volumes and Performing Actions on Them,” on page 106
- Section 13.3, “Generating Inventories for Directories or NCP Volumes,” on page 115
- Section 13.4, “Generating a Custom Inventory Report from a File Inventory Report,” on page 121
- Section 13.5, “Performing Actions on Files from Custom Reports,” on page 122
- Section 13.6, “Generating and Viewing NCP Trustee Reports for NSS Volumes,” on page 123

13.1 Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux

- Section 13.1.1, “NCP Volumes (NCP Shares),” on page 101
- Section 13.1.2, “NCP Server Parameters,” on page 102
13.1.1 **NCP Volumes (NCP Shares)**

Table 13-2 describes the management tasks available for the Manage NCP Services > Manage Shares task in Novell Remote Manager for Linux.

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
</table>
| Share Name link   | **Browse files and directories.**  
                    | View and set file system attributes for files and directories on NSS volumes.  
                    | View file information.  
                    | View directory information. |
| Mount/Unmount     | **Mount NCP volumes and NSS volumes to make them available to NCP clients.**  
                    | **Unmount NCP volumes and NSS volumes to make them unavailable to NCP clients.**          |
| Info icon         | **NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics.**  
                    | **Open files listed for each NCP connection.**  
                    | **Add a shadow volume for the NCP volume.**  
                    | For unmounted DST shadow volumes, click the Info icon to remove the shadow volume relationship. Removing a shadow volume removes the entry in the `ncpserv.conf` file, but does not delete the volumes that make up the shadow volume. |
| Create new share  | **Creates an NCP volume name (share) on a Linux POSIX file system (Ext3, XFS, or Reiser), and associates it to a path on your server. You are prompted for a volume (share) name and a path to the volume. This creates a mount point to the volume you specify and makes it accessible to NCP clients.**  
                    | **IMPORTANT:** You cannot use this method to create an NSS volume. You must use NSS tools to create and manage NSS volumes on Linux. |
| Delete existing share | **Removes the NCP volume and path association for NCP volumes on Linux POSIX file systems (Ext3, XFS, or Reiser). This does not remove or delete data from the directory; it removes only the volume mount point that was created for the NCP share.** |
### 13.1.2 NCP Server Parameters

Table 13-3 describes the management task available for the Manage NCP Services > Manager Server task in Novell Remote Manager for Linux.

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCP/NSS bindings</td>
<td>View or modify whether NSS volumes are NCP accessible. If they are not accessible, the <code>EXCLUDE_VOLUME volumename</code> command is added to the <code>/etc/opt/novell/ncp2nss.conf</code> file. Use this option for NSS volumes on clusters where the load script handles NCP mount of NSS volumes. Use this option for NSS volumes that you want to use as the secondary storage area in a Dynamic Storage Technology shadow volume.</td>
</tr>
</tbody>
</table>

### 13.1.3 NCP Server Connections

Table 13-4 describes the management tasks available for the Manage NCP Services > Manage Connections task in Novell Remote Manager for Linux.

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subtasks</td>
<td>Management Tasks</td>
</tr>
<tr>
<td>Server Parameter Information</td>
<td>View NCP Server parameters for the SET command and their current values. Click the Parameter Value link to modify the value. For a list of parameters and their default values, see “Configuring Global NCP Server Parameters” in the OES 2015 SP1: NCP Server for Linux Administration Guide.</td>
</tr>
<tr>
<td>Connection information</td>
<td>View connection statistics. Clear all Not Logged In connections.</td>
</tr>
<tr>
<td>Connection listing</td>
<td>View a list of connections. Click the name link for the connection to view statistics for the connection and a list of its open files. Clear selected connections.</td>
</tr>
<tr>
<td>Name link for the connection</td>
<td>View statistics for the connection. View the network address, status, privileges, and security equivalence for a logged-in-user. Send a message to the selected connection.</td>
</tr>
</tbody>
</table>
13.1.4 NCP Trustee Reports

Table 13-5 describes the management tasks available for the Manage NCP Services > View Trustee Reports task in Novell Remote Manager for Linux.

Table 13-5 Manage NCP Services > View Trustee Reports

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast messages to everyone</td>
<td>Broadcast messages to all logged-in NCP users. The DISABLE_BROADCAST parameter must be disabled (value of 0) in order for broadcast messages to be sent. Users must be using a Novell Client version that supports receiving broadcast messages, and the client must be configured to receive messages.</td>
</tr>
</tbody>
</table>

13.1.5 NCP Logs and Audit Logs

Table 13-6 describes the management tasks available for the Manage NCP Services > View Logs task in Novell Remote Manager for Linux.

Table 13-6 Manage NCP Services > View Logs

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logs</td>
<td>Download and view the ncpser.log and ncp2nss.log.</td>
</tr>
</tbody>
</table>
13.1.6 NCP Server Statistics

Table 13-7 describes the management tasks available for the Manage NCP Services > View Statistics task in Novell Remote Manager for Linux.

Table 13-7  Manage NCP Services > View Statistics

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit logs</td>
<td>Download and view the following audit logs:</td>
</tr>
<tr>
<td></td>
<td>• ncpsserv.audit.log</td>
</tr>
<tr>
<td></td>
<td>All the operations performed by NCP Engine are logged into this file in XML format. For example, add trustee, remove trustee, volume mount and dismount, NSS event handler startup/shutdown, add/remove volume, create shadow volume, security sync, and kill NCP connections. No file operations are logged in this file.</td>
</tr>
<tr>
<td></td>
<td>• ncp2nss.audit.log</td>
</tr>
<tr>
<td></td>
<td>The following ncp2nss events are logged into this file:</td>
</tr>
<tr>
<td></td>
<td>Open command file, write command file, ncp2nss daemon halted, ncp2nss daemon running, NSS not detected, domain socket not created, domain socket not accessible, uneb not started, failed to import uneb symbols, failed to create uneb processing thread, ndp library not started, failed to import ndp library symbols, and failed to initialize ndp library.</td>
</tr>
<tr>
<td></td>
<td>• SYS.audit.log</td>
</tr>
<tr>
<td></td>
<td>• volumename.audit.log (an audit log is listed for each NSS volume)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server information</td>
<td>View server name, server version, and product version.</td>
</tr>
<tr>
<td></td>
<td>View the number of connections.</td>
</tr>
<tr>
<td>Server statistics</td>
<td>View server statistics such as up time, traffic, and caching memory use.</td>
</tr>
</tbody>
</table>

13.1.7 NCP Server Diagnostics

Table 13-8 describes the management tasks available for the Manage NCP Services > Diagnostic Information task in Novell Remote Manager for Linux.

Table 13-8  Manage NCP Services > Diagnostic Information

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCP engine</td>
<td>View statistics for NCP events.</td>
</tr>
<tr>
<td></td>
<td>Click the Process ID (PID) link to view information about the currently running process.</td>
</tr>
</tbody>
</table>
### Dynamic Storage Technology

Table 13-9 describes the management tasks available for the View File Systems > Dynamic Storage Technology Options task in Novell Remote Manager for Linux.

**Table 13-9  View File Systems > Dynamic Storage Technology Options**

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSS interface daemon</td>
<td>View statistics for NSS events.</td>
</tr>
<tr>
<td></td>
<td>Click the Process ID (PID) link to view information about the currently running process.</td>
</tr>
<tr>
<td>Volume information</td>
<td>View a list of NCP volumes and NSS volumes on the server.</td>
</tr>
<tr>
<td></td>
<td>Click the Add Shadow link next to an NSS volume to view share information, where you can create a shadow volume. (NCP volumes are not supported as shadow volumes.)</td>
</tr>
<tr>
<td></td>
<td>Click the Inventory link next to a shadow volume to view an inventory report for both the primary and secondary volumes.</td>
</tr>
<tr>
<td></td>
<td>Click the View Log link next to an NSS volume to download a copy of the audit log for the selected volume.</td>
</tr>
<tr>
<td>Add Shadow link</td>
<td>This option takes you to the Share Information page. Scroll down to the Volume Tasks area to find the Add Shadow Volume task.</td>
</tr>
<tr>
<td></td>
<td>The Share Information page and Add Shadow Volume page do not distinguish or validate whether the volumes you choose are actually supported file systems and available combinations.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING:</strong> NSS volumes must already exist when you create the shadow volume. The Create if not present option is available for future support of NCP volumes on Linux file systems. Do not use this option for NSS volumes.</td>
</tr>
<tr>
<td>Inventory link</td>
<td>View statistics and graphical trend displays for the volume’s files and directories. For a DST shadow volume, the report includes information for both the primary storage area (primary area) and the secondary storage area (shadow area).</td>
</tr>
<tr>
<td>Volume information (Info icon)</td>
<td>NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics.</td>
</tr>
<tr>
<td></td>
<td>Open files listed for each NCP connection.</td>
</tr>
<tr>
<td></td>
<td>Add a shadow volume for the NCP volume.</td>
</tr>
<tr>
<td></td>
<td>For unmounted DST shadow volumes, click the Info icon to access the dialog to remove the shadow volume relationship. This removes the entry in the ncpconf file, but does not delete the volume itself.</td>
</tr>
<tr>
<td></td>
<td>To unmount a shadow volume, click Manage NCP Services &gt; Manage Shares, then click Unmount option next to the shadow volume.</td>
</tr>
</tbody>
</table>
13.2 Browsing NSS Volumes and Performing Actions on Them

The NCP Server plug-in to Novell Remote Manager appears as "Manage NCP Services" in the left panel. NCP volumes and NSS volumes are listed as NCP Shares.

For detailed information about creating and managing NCP volumes, see the OES 2015 SP1: NCP Server for Linux Administration Guide.

For detailed information about creating and managing NSS volumes, see the OES 2015 SP1: NSS File System Administration Guide for Linux.

For detailed information about creating and managing Dynamic Storage Technology shadow volume pairs with NSS volumes, see the OES 2015 SP1: Dynamic Storage Technology Administration Guide.

- Section 13.2.1, “Viewing Information about an NSS Volume,” on page 106
- Section 13.2.2, “Viewing the Linux POSIX Details of an NSS Directory and Performing Specific Actions on It,” on page 108
- Section 13.2.3, “Viewing the Linux POSIX Details of a File and Performing Specific Actions on It,” on page 109
- Section 13.2.4, “Browsing an NSS Volume and Setting Rights and File System Attributes on Directories and Files,” on page 110
- Section 13.2.5, “Salvaging and Purging Deleted Files on an NSS Volume,” on page 114
- Section 13.2.6, “Purging a Deleted NSS Volume,” on page 114
- Section 13.2.7, “Viewing Open File Information for an NSS Volume,” on page 115

13.2.1 Viewing Information about an NSS Volume

1 In Novell Remote Manager, select Manage NCP Services > Manage Shares.
2 In the right pane, view the list of mounted NSS volumes in the Active Shares list.
3 Next to the volume name, click the **Information** icon ( ) to go to the volume’s Share Information page.

**VOLD Share Information**

<table>
<thead>
<tr>
<th>Information</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>File system path</td>
<td><code>/media/nss/VOLD</code></td>
</tr>
<tr>
<td>File system shadow path</td>
<td>n/a</td>
</tr>
<tr>
<td>Loaded name spaces</td>
<td>DOS, LONG</td>
</tr>
<tr>
<td>File system type</td>
<td>NSS</td>
</tr>
<tr>
<td>NCP volume ID</td>
<td>2</td>
</tr>
<tr>
<td>Status</td>
<td>mounted, entire, savageable, user quotas, directory quotas</td>
</tr>
<tr>
<td>Sector Size</td>
<td>512</td>
</tr>
<tr>
<td>Sectors per Cluster</td>
<td>8</td>
</tr>
<tr>
<td>Capacity</td>
<td>456.52 MB</td>
</tr>
<tr>
<td>Used space</td>
<td>592 KB</td>
</tr>
</tbody>
</table>

4 In the **Information** table, view the following information about the NSS volume:

- File system path on Linux, such as `/media/nss/VOLD`
  
  Click the link to browse the directories and files on the volume.

- File system shadow path, such as `/media/nss/SH_VOLD` (A path is displayed only when the specified NSS volume is the primary volume of a Dynamic Storage Technology shadow volume pair.)
  
  Click the link to browse the directories and files on the pair’s secondary volume.

- Loaded name spaces, such as DOS, LONG, MAC, and UNIX

- File system type (NSS)

- NCP volume ID
  
  The NCP volume ID is a value between 0 and 254 that is automatically assigned for standalone volumes, beginning with zero. The `SYS` volume is by default assigned 0, and `_Admin` is assigned 1. For shared volumes, the volume ID is specified in the cluster load script for shared volumes, beginning with 254 and down.

- Status
Identifies whether the volume is mounted/unmounted, online/offline, or in a cluster resource. It lists the NSS volume attributes that are enabled for the volume, such as Salvageable, User Quotas, Directory Quotas, and so on.

- Sector size
- Sectors per cluster
- Capacity
- Used space
- Advanced information (Click View to view.)

<table>
<thead>
<tr>
<th>Local cache</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>trustee count</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>cached files</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>evicted files</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>cached folders</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>cache retrieved</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>cache retrieved locked</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pool name</th>
<th>NSS POOL_0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool attributes</td>
<td>NSS 0x13</td>
</tr>
<tr>
<td>GUID</td>
<td>NSS e3b410d4-42f9-01e1-80-00-0c8f506d1b22</td>
</tr>
</tbody>
</table>

- Local cache
  - Trustee count
  - Cached files
  - Evicted files
  - Cached folders
  - Cache retrieved
  - Cache retrieved locked
- Pool name
- Pool attributes
- GUID
- Open File Information (Click to view.)
- Salvageable Files (Click to view.)

### 13.2.2 Viewing the Linux POSIX Details of an NSS Directory and Performing Specific Actions on It

1. Click the View File System Listing link in the navigation frame, or click a Mount Location name link on the Home page.
2. On the Directory list page, browse to the `/media/nss/<volume_name>` directory and through its subdirectories to the directory, then click the Directory Information icon to the left of the directory name.
3. On the Directory Information page that is displayed, view the information about the file:
   - Directory owner
   - Group
   - Data modified time
13.2.3 Viewing the Linux POSIX Details of a File and Performing Specific Actions on It

1 Click the View File System Listing link in the navigation frame, or click a Mount Location name link on the Home page.

2 On the Directory list page, browse to the /media/nss/<volume_name> directory and through its subdirectories to the file, then click the File Info icon to the left of the file name.

3 On the File Information page that is displayed, view the information about the file:
   - File owner
   - Group
   - Data modified time
   - Last accessed time
   - Information change time
   - Linux POSIX read/write/execute file attributes.

   **IMPORTANT:** Do not use these settings for NCP and NSS volumes. Use the NCP view of the volume to set the Novell Trustee Model attributes.

4 Perform any of the following tasks:
Edit: The Edit button is available only on simple text files or on files with the extensions listed in the /opt/novell/nrm/nrmedit.txt file. If you want to save the file with an ANSI or UTF-8 encoding, select the appropriate option and click OK.

Delete: Click Delete to delete the selected file.

Rename: Specify the full Linux path to the file, including the new file name, then click Rename.

Create Hard Link: Specify the hard link path, then click Create Hard Link.

Create Symbolic Link: Specify the symbolic link path, then click Create Symbolic Link.

13.2.4 Browsing an NSS Volume and Setting Rights and File System Attributes on Directories and Files

1 In Novell Remote Manager, select Manage NCP Services > Manage Shares.
2 In the right pane, view the list of mounted NSS volumes in the Active Shares list.
3 Click the volume Name link to view a folder list and to browse the files on the NSS file system. Click the arrows in the column headings to sort the list by name, type (file extension), size, or last modified date and time.
4 Use the links above the file list to perform the following actions on the volume:
   • Upload
   • Text Search
   • File Search
   • Inventory
      For information, see Section 13.3, "Generating Inventories for Directories or NCP Volumes," on page 115.
5 Click a directory’s Directory Information icon to view information about the directory. You can also create subdirectories.
Managing NCP Services

- Creation date and time
- Effective rights (based on the Novell Trustee Model)
- Inherited rights filter (based on the Novell Trustee Model). You can click the link to modify the rights inheritance filter settings.
- Salvageable files

6 Click a directory’s Attributes link to view or modify the NSS file system attributes that are set for the directory. Click OK to save your changes.

<table>
<thead>
<tr>
<th>Folder Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>If checked, this indicates a system file or folder.</td>
</tr>
<tr>
<td>Hidden</td>
<td>If checked, this indicates that this file or folder is excluded from normal directory searches.</td>
</tr>
<tr>
<td>Archive</td>
<td>If checked, this indicates that the file or folder needs to be archived.</td>
</tr>
<tr>
<td>Immediate Purge</td>
<td>If checked, this indicates that when this file or folder or the folder contents are deleted and are unrecoverable.</td>
</tr>
<tr>
<td>Don’t Compress</td>
<td>If checked, this indicates that this file or the contents of the folder cannot be compressed.</td>
</tr>
<tr>
<td>Don’t Migrate</td>
<td>If checked, this indicates that this file or folder cannot be migrated to near line storage.</td>
</tr>
<tr>
<td>Delete Inhibit</td>
<td>If checked, this indicates that this file or folder cannot be deleted.</td>
</tr>
<tr>
<td>Rename Inhibit</td>
<td>If checked, this indicates that this file or folder cannot be renamed.</td>
</tr>
<tr>
<td>Immediate Compress</td>
<td>If checked, this indicates that this file or the folder contents will be scheduled for compression.</td>
</tr>
</tbody>
</table>

- System
- Hidden
- Archive
- Immediate purge
- Do not compress
- Do not migrate
- Delete inhibit
- Rename inhibit
- Immediate compress

For information about the meaning and usage of NSS file system attributes for directories, see “Understanding Directory and File Attributes for NSS Volumes” in the OES 2015 SP1: File Systems Management Guide.
7 Click a file's File Information icon to view the following file information. You can also delete the file from this page by clicking Delete File.

**VOLD:/SLES-deployment_en.pdf**

[Back to directory listings for /VOLD]

<table>
<thead>
<tr>
<th>File Information</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>admin novell</td>
</tr>
<tr>
<td>Last modified date and time</td>
<td>Wed Jan 20 13:57:12 2016</td>
</tr>
<tr>
<td>Creation date and time</td>
<td>Fri Jan 28 18:43:00 2016</td>
</tr>
<tr>
<td>Last archived date and time</td>
<td>Fri Mar 30 00:00:00 1979</td>
</tr>
<tr>
<td>Effective rights</td>
<td>SRWCEMFA</td>
</tr>
<tr>
<td>Inherited rights filter</td>
<td>SRWCEMFA</td>
</tr>
<tr>
<td>Disk space in use</td>
<td>4,645,056 Bytes</td>
</tr>
</tbody>
</table>

- Owner
- Last modified date and time
- Creation date and time
- Last archived date and time
- Effective rights (based on the Novell Trustee Model)
- Inherited rights filter (based on the Novell Trustee Model). You can click the link to modify the rights inheritance filter settings.
- Disk space in use
8 Click a file’s **Attributes** link to view or modify the NSS file system attributes that are set for the file. Click **OK** to save your changes.

### Table: NSS File System Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>If checked, this indicates a system file or folder.</td>
</tr>
<tr>
<td>Hidden</td>
<td>If checked, this indicates that the file or folder is excluded from normal directory searches.</td>
</tr>
<tr>
<td>Read Only</td>
<td>If checked, this indicates that this file cannot be deleted or modified.</td>
</tr>
<tr>
<td>Archive</td>
<td>If checked, this indicates that the file or folder needs to be archived.</td>
</tr>
<tr>
<td>Immediate Purge</td>
<td>If checked, this indicates that when this file or folder or the folder contents are deleted and are unrecoverable.</td>
</tr>
<tr>
<td>Don’t Compress</td>
<td>If checked, this indicates that this file or the contents of the folder cannot be compressed.</td>
</tr>
<tr>
<td>Don’t Migrate</td>
<td>If checked, this indicates that this file or folder cannot be migrated to near line storage.</td>
</tr>
<tr>
<td>Delete Inhibit</td>
<td>If checked, this indicates that this file or folder cannot be deleted.</td>
</tr>
<tr>
<td>Rename Inhibit</td>
<td>If checked, this indicates that this file or folder name cannot be renamed.</td>
</tr>
<tr>
<td>Immediate Compress</td>
<td>If checked, this indicates that this file or the folder contents will be scheduled for compression.</td>
</tr>
<tr>
<td>Shareable</td>
<td>If checked, this indicates that this file may be used by multiple users at the same time.</td>
</tr>
<tr>
<td>Don’t SubAllocate</td>
<td>If checked, this indicates that this file may not utilize sub-allocation for space saving.</td>
</tr>
<tr>
<td>Execute Only</td>
<td>If checked, this indicates that this file may only be executed as a program, no modifications will be allowed to the file.</td>
</tr>
<tr>
<td>Transactional</td>
<td>If checked, this indicates that Transactional tracking of data will enabled.</td>
</tr>
<tr>
<td>Copy Inhibit</td>
<td>If checked, this indicates that this file may not be copied.</td>
</tr>
</tbody>
</table>

- System
- Hidden
- Read only
- Archive
- Immediate purge
- Do not compress
- Do not migrate
- Delete inhibit
- Rename inhibit
- Immediate compress
- Shareable
- Do not suballocate
- Execute only
- Transactional
- Copy inhibit

For information about the meaning and usage of NSS file system attributes for directories, see “Understanding Directory and File Attributes for NSS Volumes” in the **OES 2015 SP1: File Systems Management Guide**.
13.2.5 Salvaging and Purging Deleted Files on an NSS Volume

From an NSS volume’s Share Information page, the Salvageable File List option allows you to view a list of deleted files that are available for salvage or purge on the volume. Deleted files are available only for NSS volumes where the Salvage attribute is enabled. For information about the NSS file salvage feature, see “Volume Salvage versus File Salvage” in the OES 2015 SP1: NSS File System Administration Guide for Linux.

1 In Novell Remote Manager, select Manage NCP Services > Manage Shares.
2 In the right pane, view the list of mounted NSS volumes in the Active Shares list.
3 Next to the volume name, click the Information icon (I) to go to the volume’s Share Information page.
4 Below the Information table, click Salvageable File List to open the Salvage File Information page.

Salvage File Information

Salvageable files

<table>
<thead>
<tr>
<th>Salvage</th>
<th>Purge</th>
<th>Name</th>
<th>Size</th>
<th>Last modified date and time</th>
<th>Deleter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salvage</td>
<td>Purge</td>
<td>SLESinstallclient.pdf</td>
<td>444KB</td>
<td>Mon Jun 20 13:57:12 2016</td>
<td>admin.novell</td>
</tr>
</tbody>
</table>

5 Salvage or purge files in the list:

If the deleted file resided in a directory that has been deleted, you must first salvage the deleted directories in the path. Salvage each lower directory in turn until you have salvaged the deleted directory that contained the file. You can then search for the deleted file in the salvaged directory.

- The Purge all files option allows you to purge all deleted files on the selected volume.
- The Salvage option allows you to recover a deleted file.
- The Purge option allows you to purge a deleted file.

You can also select a deleted directory and use this option to purge the deleted directory and all of the deleted subdirectories and files that it contains.

13.2.6 Purging a Deleted NSS Volume

For volume salvage, the NSS volumes are automatically retained on deletion. The deleted volume can be salvaged for a period of time that is determined by the server-level Logical Volume Purge Delay setting. Administrators with the Supervisor right can salvage or purge deleted volumes at any time before the purge delay elapses. For information about the NSS volume salvage feature, see “Volume Salvage versus File Salvage” in the OES 2015 SP1: NSS File System Administration Guide for Linux.

1 In Novell Remote Manager, select Manage NCP Services > Manage Shares.
2 In the right pane, view the list of mounted NSS volumes in the Active Shares list.
3 Next to the volume name, click the Information icon (I) to go to the volume’s Share Information page.
4 Scroll down to the Volume Tasks table, then click Purge Volume.
13.2.7 Viewing Open File Information for an NSS Volume

1. In Novell Remote Manager, select Manage NCP Services > Manage Shares.
2. In the right pane, view the list of mounted NSS volumes in the Active Shares list.
3. Next to the volume name, click the Information icon (I) to go to the volume’s Share Information page.
4. Below the Information table, click Open File Information to open the Open File Information page.
5. View the following information about files on the NSS volume:
   - Connection
     For information, see “Managing Connections for NCP Volumes and NSS Volumes” in the OES 2015 SP1: NCP Server for Linux Administration Guide.
   - User name
   - Open file list

13.3 Generating Inventories for Directories or NCP Volumes

With this feature, you can inventory NCP mounted volumes or general file system directories. You can also view graphs, profiles, reports, and key statistics about each of these items, including space usage trends.

Generating this report can take a while, depending on the number of files and folders in the specified directory path.

With a few clicks, you get available space trend graphs; profiles for file types, file owner, last accessed, last modified, creation time, and file size; and links to specific reports for each of these. You can also customize the scan to look for specific file information.

The File Owner Profile gathers the ownership statistics from the NSS management interface. If the eDirectory user name is available from the NSS management interface, the file owner is reported as the eDirectory user name, such as jsmith. Otherwise, the owner is reported as the nobody user. It is not required that you enable the users with Linux User Management (LUM) to get the file owner’s name.

**NOTE:** If AD users are assigned as trustees, then the file owner is reported as the Unknown user.

This section includes the following tasks:

- Section 13.3.1, “Generating a File Inventory Report,” on page 116
- Section 13.3.2, “Generating an NCP Volume Inventory Report,” on page 118
- Section 13.3.3, “Viewing a Saved NCP Inventory Report,” on page 120
- Section 13.3.4, “Emailing a Saved NCP Inventory Report (OES 11 SP1),” on page 120
13.3.1 Generating a File Inventory Report

To generate an inventory report for an entire server or any subdirectory, including mounted NCP volumes:

1 Click View File System > General File System Inventory.
   
   You can also click the Inventory link at the top of the View File System Listing page, and on subsequent pages as you navigate through the file system subdirectories.
   
   This opens the General File Inventory page. By default, the / (root) directory is selected.

2 From this point, you can do the following:
   
   Click the Start Scan button to generate an inventory of the entire server (the default selection is the / [root] subdirectory).
   
   or
   
   Select a subdirectory to generate a report from. Click the subdirectory_name links until the desired subdirectory appears in the Scan field, then click the Start Scan button.

General File Inventory

Choose Subdirectory to Inventory:

   Select /etc/xinetd.d

Browse Subdirectories:

- -
If you are viewing the File System Listing page for the desired directory, you can generate the same reports by clicking the **Inventory** link on this page.

A report similar to the following is generated:

**General File Inventory**

![Graph showing File Scanned]

**Inventory Report for: /etc/xinetd.d**

Report generated on **Mon Jul 18 17:33:01 2016**

Elapsed Time(seconds): 0

- File type profiles
- File ownership profiles
- Last modified profiles
- Last accessed profiles
- Change time profiles
- File size profiles
- Links to specific reports
- Custom Directory Tree Scan

**File Types (By Bytes In Use)**

![Graph showing File Types]

At this point, you can click any of the links to the left of the **Key Statistics** table to move quickly to the generated information, or you can create a custom report. See “Generating a Custom Inventory Report from a File Inventory Report” on page 121.
13.3.2 Generating an NCP Volume Inventory Report

1 Use either of the following methods to generate an NCP Volume Inventory Report:

- Select Manage NCP Services > Volume Inventory Reports, locate the NSS volume in the list, then click Create in the Generate Report column for the volume.

- Select View File System > NCP Volume Inventory, then select the name link of an available NCP volume in the list.

This opens the Volume Inventory page that shows all of the mounted NCP and NSS volumes available for inventory.
2 View the generated report.

A report similar to the following is generated:

```
Volume Inventory

Files Scanned
0 50 100 150 200 250 300 350 400

Inventory Report for: /usr/novell/sys
Elapsed Time(seconds): 0

File type profiles
File owner profiles
Last modified profiles
Last accessed profiles
Change time profiles
File size profiles
Links to specific reports
Custom Directory Tree Scan

File type profiles:
Data Tables:

File Types (By Bytes In Use)

At this point, you can click any of the links to the left of the Key Statistics table to move quickly to the generated information, or you can create a custom report. See “Generating a Custom Inventory Report from a File Inventory Report” on page 121.
13.3.3 Viewing a Saved NCP Inventory Report

An inventory report is saved when you run an inventory on an NCP volume.

To view the last saved report:

1. Go to the Manage NCP Services > Volume Inventory Reports page.
2. Click the View Last Report > Display option for the volume.

The saved report provides the same statistics as running View File Systems > NCP Volumes Inventory. Graphics are not available in a saved report.

13.3.4 Emailing a Saved NCP Inventory Report (OES 11 SP1)

In OES 11 SP1 and earlier, you can use the Send option in the Email Report column to send an NSS volume’s last saved NCP inventory report to addresses that are configured in the /etc/opt/novell/httpstkd.conf file. For information about setting up email addresses for Novell Remote Manager, see Section A.3, “Email Notification Commands (OES 11 SP1 and Earlier),” on page 156.

**IMPORTANT:** The Novell Remote Manager email notification system is not available in OES 2015 SP1.

To send the report:

1. Go to the Manage NCP Services > Volume Inventory Reports page.
2. In the Email Report column, click the Send option for the volume.
### 13.4 Generating a Custom Inventory Report from a File Inventory Report

After generating an inventory report for a volume or directory, you can create a customized scan to report more specific information and perform additional actions on the files selected in the report, such as move, copy, or delete.

1. Create the initial report as specified in "Generating a File Inventory Report" on page 116.
2. In the generated report, click the **Custom Directory Tree Scan** link.
   
   A page similar to the following is returned:

   ```
   Custom Directory Tree Scan
   Search Pattern: *
   File Owner Restriction: None
   Time Stamp Restrictions:
   
   Time Stamp:
   - Last Modified Time
   - Last Accessed Time
   - Last Changed Time

   Range:
   - Within Last Day
   - 1 Day - 1 Week
   - 1 Week - 2 Weeks
   - 2 Weeks - 1 Month
   - 1 Month - 2 Months
   - 2 Months - 4 Months
   - 4 Months - 6 Months
   - 6 Months - 1 Year
   - 1 Year - 2 Years
   - More than 2 Years

   File Size Restriction:
   - Less than 1KB
   - 1KB - 4KB
   - 4KB - 16KB
   - 16KB - 64KB
   - 64KB - 256KB
   - 256KB - 1MB
   - 1MB - 4MB
   - 4MB - 16MB
   - 16MB - 64MB
   - 64MB - 256MB
   - More than 256MB
   
   Start Scan
   ```

3. Type the specific search criteria in the **Search Pattern** field.
   
   `*.*` is the default entry.

4. Select the desired settings in the **File Owner Restriction** drop-down box.
   
   **None** is the default selection.

5. Select the check boxes desired to customize the report by **Time Stamp** or **File Size** restrictions.
   
   No restrictions is the default setting.
13.5 Performing Actions on Files from Custom Reports

After a custom report is generated, you can perform the following actions on the files listed in the report for the selected volume.

- Section 13.5.1, “Moving Selected Files,” on page 122
- Section 13.5.2, “Copying Selected Files,” on page 122
- Section 13.5.3, “Deleting Selected Files,” on page 123
- Section 13.5.4, “Opening or Downloading a File,” on page 123
- Section 13.5.5, “Managing Individual Files,” on page 123

13.5.1 Moving Selected Files

1. From the generated report, select the check box to the left of each file that you want to move. To move all files in the list, click the Check All button.

2. Specify the path where you want to move the selected files in the field to the right of the Move Checked File To button.
   
   The target path must be to a location on the same volume.

3. Click the Move Checked File To button.

13.5.2 Copying Selected Files

1. From the generated report, select the check box to the left of each file that you want to copy. To copy all files in the list, click the Check All button.

2. Specify the path where you want to copy the selected files in the field to the right of the Copy Checked File To button.
Managing NCP Services

13.5.3 Deleting Selected Files

1. From the generated report, select the check box to the left of each file that you want to delete. To delete all files in the list, click the Check All button.
2. Click the Delete Checked Files button.

13.5.4 Opening or Downloading a File

1. From the generated report, select the file_name link for the file you want to open or download.
2. From the resulting dialog box, select Open With or Save to Disk, then click OK.

13.5.5 Managing Individual Files

1. From the generated report, click the File Information icon.
2. To perform the desired action (edit, delete, rename, create hard link, or create symbolic link) for the file, specify the required information in the applicable field, then click the applicable button.

   The target path for the action must be to a location on the same volume.

13.6 Generating and Viewing NCP Trustee Reports for NSS Volumes

Under Manage NCP Services, the View Trustee Reports option opens the NCP Trustee Reports page where you can generate a trustee report for a specified NSS volume. This includes Dynamic Storage Technology shadow volumes that are comprised of two NSS volumes. You can display the last trustee report in the web browser. A trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume.

In OES 11 SP1 and earlier, you can also send the report to the email addresses that you have pre-configured for Novell Remote Manager.

- Section 13.6.1, “Generating an NCP Trustee Report,” on page 124
- Section 13.6.2, “Viewing a Saved NCP Trustee Report,” on page 124
- Section 13.6.3, “Emailing a Saved NCP Trustee Report (OES 11 SP1),” on page 124
13.6.1 Generating an NCP Trustee Report

1. Log in to Novell Remote Manager as the root user.
2. In the left navigation panel, select Manage NCP Services > View Trustee Reports to open the NCP Trustee Reports page.

<table>
<thead>
<tr>
<th>Volume</th>
<th>View Last Report</th>
<th>Generate Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3</td>
<td>Display</td>
<td>Create</td>
</tr>
<tr>
<td>V2</td>
<td>Display</td>
<td>Create</td>
</tr>
<tr>
<td>V1</td>
<td>Display</td>
<td>Create</td>
</tr>
</tbody>
</table>

3. On the NCP Trustee Reports page, locate the NSS volume in the list, then click its Create link in the Generate Report column.
4. View the NCP Trustee Report.

A volume’s trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume. For example, the following trustee report shows the rights for a folder in a Dynamic Storage Technology shadow volume.

**Shadow Volume Trustee Report**

Primary Volume Tree: /media/nss/V1
Shadow Volume Tree: /media/nss/V1SHADOW

/media/nss/V1/folder/jim

Elapsed Time(seconds): 14

13.6.2 Viewing a Saved NCP Trustee Report

You can view the last saved trustee report for an NSS volume. The saved report provides the same trustee rights information that was available when the report was created.

1. Log in to Novell Remote Manager as the root user.
2. In the left navigation panel, select Manage NCP Services > View Trustee Reports.
3. Locate the NSS volume of interest in the list, then click its Display link in the View Last Report column.

13.6.3 Emailing a Saved NCP Trustee Report (OES 11 SP1)

In OES 11 SP1 and earlier, you can use the Send option in the Email Report column to send an NSS volume’s last saved NCP trustee report to addresses that are configured in the /etc/opt/novell/httpstkd.conf file. For information about setting up email addresses for Novell Remote Manager, see Section A.3, “Email Notification Commands (OES 11 SP1 and Earlier),” on page 156.

**IMPORTANT:** The Novell Remote Manager email notification system is not available in OES 11 SP2 and later.
To send a saved report:

1. Log in to Novell Remote Manager as the root user.
2. In the left navigation panel, select Manage NCP Services > View Trustee Reports.
3. Locate the NSS volume of interest in the list, then click its Send link in the Email Report column.
Managing Dynamic Storage Technology Options

This section provides an overview of tasks that can be performed when the NCP Server and Dynamic Storage Technology plug-in is installed in Novell Remote Manager.

For information about using and managing Dynamic Storage Technology on Open Enterprise Server (OES) 2015 SP1, see the OES 2015 SP1: Dynamic Storage Technology Administration Guide.

For information about using and managing NSS volumes on OES 2015 SP1, see the OES 2015 SP1: NSS File System Administration Guide for Linux.

The View File System > Dynamic Storage Technology Options section in Novell Remote Manager for Linux includes the following links to these pages:

<table>
<thead>
<tr>
<th>Link</th>
<th>Actions</th>
</tr>
</thead>
</table>
| View File Systems > Dynamic Storage Technology Options > Volume Information | Volume Share Information  
  • View file system shadow path  
  • Add shadow volume  
  See “Adding a Shadow to the Primary NSS Volume (Linking the NSS Volumes)” in the OES 2015 SP1: Dynamic Storage Technology Administration Guide. |
| View File Systems > Dynamic Storage Technology Options > Shadow Status |  
  • Shadowed  
  • Add Shadow  
  See “Adding a Shadow to the Primary NSS Volume (Linking the NSS Volumes)” in the OES 2015 SP1: Dynamic Storage Technology Administration Guide. |
<p>| View File Systems &gt; Dynamic Storage Technology Options &gt; Inventory | Inventory creates inventory for the primary volume, secondary volume, and merged view of volumes. See “Generating a File Inventory for DST Shadow Volumes” in the OES 2015 SP1: Dynamic Storage Technology Administration Guide. |</p>
<table>
<thead>
<tr>
<th>Link</th>
<th>Actions</th>
</tr>
</thead>
</table>
| View File Systems > Dynamic Storage Technology Options > Dynamic Storage Technology Policies | • View a list of DST policies.  
• View summary information about when it was last executed and the total files moved.  
• Select the policy to view or modify the policy settings.  
• Select the policy, scroll to the bottom of the Policy page, then click Delete.  
| View File Systems > Dynamic Storage Technology Options > Stop all running policies | See “Stopping a Running Policy” in the OES 2015 SP1: Dynamic Storage Technology Administration Guide. |
| View File Systems > Dynamic Storage Technology Options > Duplicate file resolution options | • Broadcast conflict message to user  
• Action to be taken  
  • Show duplicate shadow files (default)  
  • Hide duplicate shadow files  
  • Rename duplicate shadow files  
  • Delete duplicate files from shadow area  
  • Move duplicate shadow files to /._DUPLICATE_FILES  
See “Resolving Instances of Duplicate Files” in the OES 2015 SP1: Dynamic Storage Technology Administration Guide. |
| Manage NCP Services > Manage Shares > NCP Shares | NCP Shares  
• NCP/NSS bindings  
• Volume Information > Volume Tasks > Add Shadow Volume  
• Unmount > Volume Information > Volume Tasks > Remove Shadow  
For information about adding and removing shadow volume pairs, see “Creating and Managing DST Shadow Volumes for NSS Volumes” in the OES 2015 SP1: Dynamic Storage Technology Administration Guide. |
Link | Actions
--- | ---
Manage NCP Services > Manage Server | NCP Manage Server

- Global policy parameters for Dynamic Storage Technology

  DUPLICATE_SHADOW_FILE_ACTION
  DUPLICATE_SHADOW_FILE_BROADCAST
  REPLICATE_PRIMARY_TREE_TO_SHADOW
  SHIFT_ACCESSSED_SHADOW_FILES
  SHIFT_DAYS_SINCE_LAST_ACCESS
  SHIFT_MODIFIED_SHADOW_FILES

For more information about how these settings affect shadow volume pairs on the server, see "Configuring DST Global Policies" in the OES 2015 SP1: Dynamic Storage Technology Administration Guide.
Managing CIFS Services

The CIFS-NRM plug-in to Novell Remote Manager allows you to manage connections and open files on NSS volumes for a CIFS server. When you install Novell CIFS, the plug-in adds the Manage CIFS Services section in NRM. With the file monitoring options, you can view details of open files and close open files by connection or by file. The tasks can be performed on NSS volumes where you have configured CIFS shares by using Novell CIFS.

For information about using and managing CIFS services on Novell Open Enterprise Server (OES) 2015 SP1, see the OES 2015 SP1: Novell CIFS for Linux Administration Guide.

For information about using and managing NSS volumes on OES 2015 SP1, see the OES 2015 SP1: NSS File System Administration Guide for Linux.

The Manage CIFS Services section includes the following links to CIFS server management pages:

Table 15-1  Links for Manage CIFS Services

<table>
<thead>
<tr>
<th>Link</th>
<th>Page Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Connections</td>
<td>CIFS Connections</td>
</tr>
<tr>
<td>View Logs</td>
<td>CIFS System Logs</td>
</tr>
<tr>
<td></td>
<td>* libnrm2cifs.log</td>
</tr>
<tr>
<td></td>
<td>* cifs.log</td>
</tr>
<tr>
<td>Manage Open Files</td>
<td>CIFS Open File Management</td>
</tr>
<tr>
<td></td>
<td>* Connection information (statistics)</td>
</tr>
<tr>
<td></td>
<td>* Connection listing</td>
</tr>
<tr>
<td></td>
<td>* Detailed information about a connection, including open files</td>
</tr>
</tbody>
</table>

From these pages you can perform the following tasks:

- Section 15.1, “Managing CIFS Connections,” on page 131
- Section 15.2, “Viewing Log Information,” on page 132
- Section 15.3, “Managing Open Files,” on page 132

15.1  Managing CIFS Connections

By querying or listing all open connections, you can understand how many sessions are opened at any moment. The details for each connection include the session ID, client IP address, user name, user login time, consolidated list of read/write requests, access mode, and total number of other requests received. You can drill-down to extract per-connection details, such as the group that the user is a member of.
Table 15-2  CIFS Connection Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access mode</td>
<td>Indicates the mode in which the CIFS server has opened the file on behalf of the user. This field displays information that the CIFS server has interpreted from the data received as part of both the Access Mask field and the Share Access field in the SMB_COM_NT_CREATE_ANDX request.</td>
</tr>
<tr>
<td>DD</td>
<td>Indicates that the right to delete or rename the file is denied for all other connections.</td>
</tr>
<tr>
<td>Desired access</td>
<td>Specifies the access modes that the client has requested.</td>
</tr>
<tr>
<td>DR</td>
<td>Indicates that the right to read data from the file is denied.</td>
</tr>
<tr>
<td>DW</td>
<td>Indicates that the right to write data into the file is denied.</td>
</tr>
<tr>
<td>ND</td>
<td>Indicates that the right to delete or rename the file is denied for this connection.</td>
</tr>
<tr>
<td>RD</td>
<td>Indicates that the right to read data from the file is granted.</td>
</tr>
<tr>
<td>Shared access</td>
<td>Specifies the sharing modes that the client has requested; that is, how the file should be shared with other users.</td>
</tr>
<tr>
<td>WR</td>
<td>Indicates that the right to write data into the file is granted.</td>
</tr>
</tbody>
</table>

1 Log in to Novell Remote Manager as the root user.
2 Click Manage CIFS Services > Manage Connections to display the CIFS Connections page.
3 You can perform the following tasks for open connections on a CIFS server:
   • Status of Open Connections: The CIFS Connection List table displays the connection number, name of user accessing the connection, reads and writes for each connection, CIFS requests by each connection, login details for the connection, and connection type to view CIFS connections for both Active Directory users and eDirectory users.
   • View Connection Information: Click the connection name to view more details for a specific connection.

15.2 Viewing Log Information

1 Log in to Novell Remote Manager as the root user.
2 Click Manage CIFS Services > View Logs to display the CIFS System Logs page.
3 You can view the following logs for the CIFS server:
   • libnrm2cifs.log: Logs debug messages associated with the CIFS-NRM plug-in. Click the file to view the messages.
   • cifs.log: Logs information, warning, and error messages associated with the CIFS server. Click the file to view the messages.

15.3 Managing Open Files

You can use the file listing options to view the following information:
   • All open files for a particular NSS volume
• All open files by a connection
• All users who have open file handles for a particular file

You can use the file closing options to close the following:

• All open files for a particular NSS volume
• All open files by a particular connection
• All open file handles associated with a particular file

If the user tries to perform any operation on an open file that was closed by using the management tool, the changes might appear the next time the file is opened, depending on the application. However, the data that was saved before the file is closed will be intact.

**WARNING:** Administrative closure is not the recommended way to close files. It is provided as a tool to administrators to force close files.

1. Log in to Novell Remote Manager as the root user.
2. Click Manage CIFS Services > Manage Open Files to display the CIFS Open File Management page.
3. The CIFS Volume lists the mounted NSS volumes.
4. You can perform the following tasks for files that are open on the selected NSS volume:
   • **Status of Open Files:** The List of Open Files table displays the connection number, name of user accessing the file, and path of the file. The files are listed for the selected NSS volume. You can also set a filter for displaying the specific file type for that volume.
   • **Close Files:** Select the files you want to close, then click Close. This closes the file immediately and allows no other file operations to be performed. Ensure that you inform the user before closing the file, to allow the user time to save the file; otherwise, the user might lose unsaved data for the file.
Managing AFP Services

The AFP-NRM plug-in to Novell Remote Manager allows you to manage connections and open files on NSS volumes for AFP server. When you install Novell AFP, the plug-in adds the Manage AFP Services section in NRM. You can close connections that are stale and persistent. With the file monitoring options, you can view details of open files and close open files by connection or by file. The tasks can be performed on NSS volumes where you have configured AFP shares by using Novell AFP.

For information about using and managing AFP services on Open Enterprise Server (OES) 2015 SP1, see the OES 2015 SP1: Novell AFP for Linux Administration Guide.

For information about using and managing NSS volumes on OES 2015 SP1, see the OES 2015 SP1: NSS File System Administration Guide for Linux.

The Manage AFP Services section includes the following links to AFP server management pages:

Table 16-1 Links for Manage AFP Services

<table>
<thead>
<tr>
<th>Link</th>
<th>Page Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Connections</td>
<td>AFP Connections</td>
</tr>
<tr>
<td>View Logs</td>
<td>AFP System Logs</td>
</tr>
<tr>
<td></td>
<td>• afptcp.log</td>
</tr>
<tr>
<td></td>
<td>• libnrm2afp.log</td>
</tr>
<tr>
<td>Manage Open Files</td>
<td>AFP Open File Management</td>
</tr>
<tr>
<td></td>
<td>• Connection information (statistics)</td>
</tr>
<tr>
<td></td>
<td>• Connection listing</td>
</tr>
<tr>
<td></td>
<td>• Detailed information about a connection, including open files</td>
</tr>
</tbody>
</table>

From these pages you can perform the following tasks:

- Section 16.1, “Managing AFP Connections,” on page 136
- Section 16.2, “Viewing Log Information,” on page 136
- Section 16.3, “Managing Open Files,” on page 137
16.1 Managing AFP Connections

By querying or listing all open connections, you can understand how many sessions are opened at any moment. The details for each connection include the session ID, client IP address, user name, user login time, consolidated list of read/write requests, access mode, and total number of other requests received. You can drill down to extract per-connection details, such as the group that the user is a member of.

If the connections are stale and persistent (for example, if there is no activity for a considerable amount of time), this session occupies a considerable chunk of memory. In this scenario, the administrator can close the connection/session based on the qualitative analysis of various connection parameters dumped by the new commands/options that are introduced.

Table 16-2  AFP Connections Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access mode</td>
<td>Indicates the mode in which the AFP server has opened the file on behalf of the user.</td>
</tr>
<tr>
<td>DD</td>
<td>Indicates that the right to delete or rename the file is denied for all other connections.</td>
</tr>
<tr>
<td>Desired access</td>
<td>Specifies the access modes that the client has requested.</td>
</tr>
<tr>
<td>DR</td>
<td>Indicates that the right to read data from the file is denied.</td>
</tr>
<tr>
<td>DW</td>
<td>Indicates that the right to write data into the file is denied.</td>
</tr>
<tr>
<td>ND</td>
<td>Indicates that the right to delete or rename the file is denied for this connection.</td>
</tr>
<tr>
<td>RD</td>
<td>Indicates that the right to read data from the file is granted.</td>
</tr>
<tr>
<td>Shared access</td>
<td>Specifies the sharing modes that the client has requested, that is, how the file should be shared with other users.</td>
</tr>
<tr>
<td>WR</td>
<td>Indicates that the right to write data into the file is granted.</td>
</tr>
</tbody>
</table>

1. Log in to Novell Remote Manager as the root user.
2. Click Manage AFP Services > Manage Connections to display the AFP Connections page.
3. You can perform the following tasks for open connections on an AFP server:
   - **Status of Open Connections**: The AFP Connection List table displays the connection number, name of user accessing the connection, reads and writes for each connection, AFP requests by each connection, and login time details for the connection.
   - **View Connection Information**: Click the connection name to view more details of a specific connection.
   - **Close Connections**: Select the connections you want to close, then click Close. This closes the connection immediately, closes its open files, and allows no other file operations to be performed. Ensure that you close any open files before closing the associated connection; otherwise, the user might lose unsaved data for the file.

16.2 Viewing Log Information

1. Log in to Novell Remote Manager as the root user.
2. Click Manage AFP Services > View Logs to display the AFP System Logs page.
You can view the following logs for an AFP server:

- **libnrm2afp.log**: Logs debug messages associated with the AFP-NRM plug-in. Click the log file to view the messages.
- **afptcp.log**: Logs status, debug, and error messages associated with the AFP server. Click the log file to view the messages.

### 16.3 Managing Open Files

You can use the file listing options to view the following information:

- All open files for a particular NSS volume
- All open files by a connection
- All users who have open file handles for a particular file

You can use the file closing options to close the following:

- All open files for a particular NSS volume
- All open files by a particular connection
- All open file handles associated with a particular file

If the user tries to perform any operation on an open file that was closed by using the management tool, the changes might appear the next time the file is opened, depending on the application. However, the data that was saved before the file is closed will be intact.

**WARNING:** Administrative closure is not the recommended way to close files. It is provided as a tool to administrators to force close files.

1. Log in to Novell Remote Manager as the **root** user.
2. Click **Manage AFP Services > Manage Open Files** to display the AFP Open File Management page.
3. You can perform the following tasks for open files on an AFP server:

   - **Status of Open Files**: The **List of Open Files** table displays the connection number, name of the user accessing the file, and path of the file. The files are listed for the selected NSS volume. You can also set a filter for displaying the specific file type for that volume.

   - **Close Files**: Select the files you want to close, then click **Close**. This closes the file immediately and allows no other file operations to be performed. Ensure that you inform the user before closing the file, to allow the user time to save the file; otherwise, the user might lose unsaved data for the file.
The following table provides information about specific tasks you can perform using Novell Remote Manager. These references also link to more specific information in this guide.

**Table 17-1 Task Quick Reference List**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Link in Navigation frame or Other Location</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build a group for monitoring</td>
<td>Use Group Operations &gt; Configure New Group</td>
<td>Building and Configuring a Monitoring Group (page 88)</td>
</tr>
<tr>
<td>Cron job, schedule</td>
<td>Manage Linux &gt; Schedule Task</td>
<td>“Scheduling cron Jobs to Run on the Server” on page 78</td>
</tr>
<tr>
<td>Directory, change attributes of</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing Details about Directories and Performing Actions on Them (page 67)</td>
</tr>
<tr>
<td>Directory, edit</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing Details about Directories and Performing Actions on Them (page 67)</td>
</tr>
<tr>
<td>Directory, delete</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing Details about Directories and Performing Actions on Them (page 67)</td>
</tr>
<tr>
<td>Directory, rename</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing Details about Directories and Performing Actions on Them (page 67)</td>
</tr>
<tr>
<td>Directory, view detailed information about</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing Details about Directories and Performing Actions on Them (page 67)</td>
</tr>
<tr>
<td>File, change attributes of</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing the Details of a File and Performing Specific Actions (page 69)</td>
</tr>
<tr>
<td>File, download</td>
<td>View File System &gt; View File System Listing</td>
<td>Downloading a File from the Server to a Local Workstation (page 68)</td>
</tr>
<tr>
<td>File, edit</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing the Details of a File and Performing Specific Actions (page 69)</td>
</tr>
<tr>
<td>File, delete</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing the Details of a File and Performing Specific Actions (page 69)</td>
</tr>
<tr>
<td>File, rename</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing the Details of a File and Performing Specific Actions (page 69)</td>
</tr>
<tr>
<td>Files, search for text in</td>
<td>View File System &gt; View File System Listing</td>
<td>Searching for Text in Files (page 69)</td>
</tr>
<tr>
<td>Tasks</td>
<td>Link in Navigation frame or Other Location</td>
<td>For More Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File, upload</td>
<td>View File System &gt; View File System Listing</td>
<td>Uploading a File to the Server (page 68)</td>
</tr>
<tr>
<td>File, view</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing Individual Files (page 70)</td>
</tr>
<tr>
<td>File system, browse</td>
<td>View File System &gt; View File System Listing</td>
<td>Browsing File Systems and Performing Actions on Them (page 65)</td>
</tr>
<tr>
<td>File system, perform action on</td>
<td>View File System &gt; View File System Listing</td>
<td>Browsing File Systems and Performing Actions on Them (page 65)</td>
</tr>
<tr>
<td>Files, viewing details about</td>
<td>View File System &gt; View File System Listing</td>
<td>Viewing the Details of a File and Performing Specific Actions (page 69)</td>
</tr>
<tr>
<td>Group operations, access an existing group</td>
<td>Use Group Operations &gt; Select Group</td>
<td>Accessing an Existing Group (page 93)</td>
</tr>
<tr>
<td>Group operations, build and configure a new monitoring group</td>
<td>Use Group Operations &gt; Configure New Group</td>
<td>Building and Configuring a Monitoring Group (page 88)</td>
</tr>
<tr>
<td>Group operations, change an existing group</td>
<td>Use Group Operations &gt; Select Group</td>
<td>Changing an Existing Group (page 93)</td>
</tr>
<tr>
<td>Group operations, define or edit Group Monitoring types</td>
<td>Use Group Operations &gt; NRM Health Types</td>
<td>Defining or Editing Group Monitoring Types (page 96)</td>
</tr>
<tr>
<td>Group operations, delete an existing group</td>
<td>Use Group Operations &gt; Select Group</td>
<td>Deleting an Existing Group (page 94)</td>
</tr>
<tr>
<td>Group operations, discover items to monitor on the network.</td>
<td>Use Group Operations &gt; Configure New Group &gt; right-click menu &gt; Network Discovery</td>
<td>Discovering Items on the Network to Monitor (page 97)</td>
</tr>
<tr>
<td>Group operations, generate and view server reports</td>
<td>Use Group Operations &gt; Configure New Group &gt; right-click menu &gt; Save Group</td>
<td>Generating and Viewing Server Reports (page 94)</td>
</tr>
<tr>
<td>Group operations, save a new group</td>
<td>Use Group Operations &gt; Configure New Group &gt; right-click menu &gt; Save Group</td>
<td>Saving a Group (page 92)</td>
</tr>
<tr>
<td>Group operations, view defined health types</td>
<td>Use Group Operations &gt; NRM Health Types</td>
<td>Viewing Group Monitoring Types (page 95)</td>
</tr>
<tr>
<td>Group operations, view monitored items</td>
<td>View Monitored Items</td>
<td>Viewing Monitored Items (page 95)</td>
</tr>
<tr>
<td>Host, shut down</td>
<td>Manage Linux &gt; Down/Reset Options</td>
<td>Shutting Down and Restarting the Host (page 74)</td>
</tr>
<tr>
<td>Host, restart</td>
<td>Manage Linux &gt; Down/Reset Options</td>
<td>Shutting Down and Restarting the Host (page 74)</td>
</tr>
<tr>
<td>Interrupt information, view</td>
<td>Manage Hardware &gt; Interrupt Information</td>
<td>Viewing Interrupt Information (page 82)</td>
</tr>
<tr>
<td>Tasks</td>
<td>Link in Navigation frame or Other Location</td>
<td>For More Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>I/O Memory information, view</td>
<td>Manage Hardware &gt; IO Memory Information</td>
<td>Viewing I/O Memory Information (page 83)</td>
</tr>
<tr>
<td>IO Port information, view</td>
<td>Manage Hardware &gt; IO Port Information</td>
<td>Viewing I/O Port Information (page 84)</td>
</tr>
<tr>
<td>Kernel modules, view</td>
<td>Manage Linux &gt; Kernel Module Listing</td>
<td>Viewing Kernel Modules (page 73)</td>
</tr>
<tr>
<td>Mounted devices, perform actions on them</td>
<td>Home icon &gt; Info icon</td>
<td>Viewing Mounted Devices and Performing Actions on Them (page 64)</td>
</tr>
<tr>
<td>Mounted devices, view</td>
<td>Home icon &gt; Info icon</td>
<td>Viewing Mounted Devices and Performing Actions on Them (page 64)</td>
</tr>
<tr>
<td>Packages, install</td>
<td>Manage Linux &gt; Package Information</td>
<td>Managing Packages (page 75)</td>
</tr>
<tr>
<td>Packages, remove</td>
<td>Manage Linux &gt; Package Information</td>
<td>Managing Packages (page 75)</td>
</tr>
<tr>
<td>Packages, view information about</td>
<td>Manage Linux &gt; Package Information</td>
<td>Managing Packages (page 75)</td>
</tr>
<tr>
<td>Partition information, view</td>
<td>View File System &gt; View Partition Information</td>
<td>Viewing Partition Information (page 70)</td>
</tr>
<tr>
<td>Process, kill</td>
<td>Manage Linux &gt; Process Information</td>
<td>Managing Processes (page 76)</td>
</tr>
<tr>
<td>Process, view information about</td>
<td>Manage Linux &gt; Process Information</td>
<td>Managing Processes (page 76)</td>
</tr>
<tr>
<td>Processors, view information about</td>
<td>Manage Hardware &gt; View Processors</td>
<td>Viewing Processors (page 81)</td>
</tr>
<tr>
<td>OES 2015 SP1 Server health</td>
<td>Diagnose &gt; Server Health Values</td>
<td>Diagnosing Problems Using Ganglia and Nagios (OES 2015 SP1) (page 39)</td>
</tr>
<tr>
<td>OES 2015 SP1 Nagios</td>
<td>Configuration Options &gt; Nagios Configuration</td>
<td>Configuring Nagios (page 47)</td>
</tr>
<tr>
<td>OES 2015 SP1 Nagios user management</td>
<td>Configuration Options &gt; Nagios Configuration &gt; Nagios User Management</td>
<td>Managing Nagios Users (page 55)</td>
</tr>
<tr>
<td>OES 2015 SP1 Nagios alert notification system for Ganglia and Nagios health alerts</td>
<td>Configuration Options &gt; Nagios Configuration</td>
<td>Modifying the Nagios Notification Methods for Contacts (page 58)</td>
</tr>
<tr>
<td>Server Group, monitor overall server health</td>
<td>Use Group Operation &gt; Configure New Group or Select Group</td>
<td>Building and Configuring a Monitoring Group (page 88)</td>
</tr>
<tr>
<td>SMBIOS information, view</td>
<td>Manage Hardware &gt; SMBIOS Information</td>
<td>Viewing SMBIOS Information (page 85)</td>
</tr>
</tbody>
</table>
18 Troubleshooting Novell Remote Manager

This section describes known issues and workarounds for Novell Remote Manager for Open Enterprise Server.

- Section 18.1, “Daemon httpstkd Is Unable to Start,” on page 143
- Section 18.2, “Error while loading shared libraries: libldapx.so.0,” on page 143
- Section 18.3, “Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 2015 SP1,” on page 144
- Section 18.4, “Ganglia Statistical Graphics Are Not Displayed in the Web Browser,” on page 145

18.1 Daemon httpstkd Is Unable to Start

The Novell Remote Manager daemon httpstkd might be unable to start if the ports it is trying to use are busy. This error is commonly shown by applications when the ports it uses (in this case NRM ports 8008 and 8009) are busy and do not respond. In this situation, you can start httpstkd without needing to reboot the server by modifying the ports used by Novell Remote Manager in the /etc/opt/novell/httpstkd.conf file:

1. Log in to the server as the root user.
2. Open the /etc/opt/novell/httpstkd.conf file in a text editor.
3. Change the default ports 8008 and 8009 to other unused ports on the following lines:
   
```
   addr 0.0.0.0:8008
   addr 0.0.0.0:8009 keyfile=/etc/opt/novell/httpstkd/server.key
certfile=/etc/opt/novell/httpstkd/server.pem
```
4. Save your changes, then close the /etc/opt/novell/httpstkd.conf file.
5. Open a terminal console, then start the httpstkd daemon by entering:

```
rcnovell-httpstkd start
```

18.2 Error while loading shared libraries: libldapx.so.0

The following error might occur during the Novell Remote Manager installation if eDirectory is not yet available:

```
Starting the Novell Small Http Interface
Daemon/opt/novell/httpstkd/sbin/httpstkd: error while loading shared libraries: libldapx.so.0: cannot open shared object file: No such file or directory
```

Httpstkd tries to start after the rpm is installed. It cannot start at that time if eDirectory has yet to be installed. When you get the Installation Completed dialog box, the httpstkd daemon is running.
18.3 Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 2015 SP1

You might see an Apache 403 Forbidden Warning error reported in Nagios after a new installation or upgrade to OES 2015 SP1.

To resolve the issue, you can try the following:

1. Log in to the server as the root user, open a terminal console, then navigate to the /etc/nagios/objects directory.

2. In the localhost.cfg file, modify the checkcommand parameters in the section, "# Define a service to check HTTP on the local machine":

   At the command prompt, enter

   ```
   define service {
     use local-service ; Name of service template to use
     host_name localhost
     service_description HTTP
     checkcommand check_http! -e 'HTTP/1.0 200','HTTP/1.1 200','HTTP/1.1 403 Forbidden'
     notifications_enabled 0
   }
   ```

3. Restart Nagios.

   `rcnagios restart`

4. After a few minutes, verify that the HTTP status for Nagios has been updated to the OK (green) state.

   4a. Log in as the root user to Novell Remote Manager.

   4b. Select Diagnose > Server Health Services, then click Nagios Service Detail.

   4c. In the Nagios Authentication Required dialog box, specify your Nagios user credentials, then click OK.

   4d. View the HTTP status in the Nagios main dashboard.
18.4 Ganglia Statistical Graphics Are Not Displayed in the Web Browser

The Novell Remote Manager frame sends secure content. However, Ganglia uses scripts to graphically display statistics that send the statistical data via HTTP instead of HTTPS. Depending on how your web browser is configured to handle mixed content on a web page, the Ganglia statistics might not be displayed in the graph windows.

- Section 18.4.1, “Firefox,” on page 145
- Section 18.4.2, “Internet Explorer,” on page 146
- Section 18.4.3, “Chrome,” on page 146

18.4.1 Firefox

In Firefox 23 and later, when you access a page with both HTTPS and HTTP content, a shield icon appears in the address bar, and the browser automatically blocks certain content such as non-secure scripts. To allow mixed content, right-click the shield icon, then select **Disable Protection on This Page**. After you disable protection, an orange alert icon appears in the address bar and makes you aware that the displayed page contains mixed content.

In a Mozilla Firefox 22 and earlier web browser, you receive a warning, but content is not automatically blocked. A **Security Warning** pop-up dialog box reports: You have requested an encrypted page that contains some unencrypted information. Click **OK** to dismiss the warning and allow mixed content to be displayed.

A round shield icon replaces the lock to the left of the https:// in the address bar. Right-click the icon to view the message that advises: Your connection to this site is only partially encrypted, and does not prevent eavesdropping.
18.4.2 **Internet Explorer**

In a Microsoft Internet Explorer web browser, the pop-up dialog box is displayed at the bottom of the page and reports: *Only secure content is displayed. Click Show all content to dismiss the warning and allow mixed content to be displayed.*

![Internet Explorer warning](image)

18.4.3 **Chrome**

In a Google Chrome web browser, a shield appears at the end of the URL in the address bar. It warns: *This page includes scripts from unauthenticated resources. Right-click the shield, then click Load Unsafe Script.*

![Chrome shield with options](image)

While mixed content is displayed in Chrome, the green text `https://` and lock in the URL `https://`, which indicates secure-only content, is automatically changed to red text that is crossed out and a gray lock with a red X `https://`. 
19 Security Considerations

This section contains information that helps you know whether you can use this utility in a secure environment and points you to information to help you set up access to your server so you can be certain that its contents are not compromised through the use of this utility.

For additional security implementation information, see “Security” in the OES 2015 SP1: Planning and Implementation Guide.

The default settings for Novell Remote Manager for OES Linux are set so your network and information cannot be compromised. If you change settings from the default, please be aware of the consequences of your actions.

- Section 19.1, “Security Features,” on page 147
- Section 19.4, “Nagios Security Configuration,” on page 151

19.1 Security Features

The following table contains the security features of Novell Remote Manager on OES Linux.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Yes/ No</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users are authenticated</td>
<td>Yes</td>
<td>Users of Novell Remote Manager must provide a user name and password credentials to log in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log in as user root, a local Linux user, or as a Novell eDirectory user that is Linux User Management enabled. The user sees only those functions that the user has permissions to view or manage.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The root user is authenticated locally, not through eDirectory. This allows the root user to manage server resources even if the eDirectory services are not available. The root user has all permissions necessary to manage all functions in Novell Remote Manager.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, see “Accessing Novell Remote Manager” on page 22 and “Changing the HTTPSTKD Configuration” on page 31.</td>
</tr>
<tr>
<td>Certificate handling by the web browser</td>
<td>Yes</td>
<td>Certificate handling requires SSL 2.0 or later, or TLS 1.0 or later, to be enabled in your web browser. Otherwise, the browser displays an error indicating that the page cannot be displayed. We recommend the higher security options of SSL 3.0, or the latest TLS if it is available.</td>
</tr>
</tbody>
</table>
Limited root user privileges for the Admin user | Yes | User root can restrict all users from logging in, so the Admin user or Admin-equivalent user is not granted unlimited root privileges for security reasons. If the server is LUM enabled, the Admin user and users with rights equivalent to the Admin user have the limited root user privileges that are needed to modify only the configuration files necessary for configuring NRM or any other files that NRM has been assigned rights to allow modifying. The user Admin or equivalent user has access according to the Linux and LUM file rights to all other files.

The Admin user or equivalent user needs root privileges to modify the following files in order to configure and manage NRM. The privileges are temporary and only for the task to be performed.

/etc/opt/novell/httpstkd.conf
/etc/pam.d/httpstkd

The following file names are the names that are used as the description for a specified task:
/etc/cron.d/[task file name]

The following files may be the actual file or a symbolic link to the YAST or eDirectory certificates:
/etc/opt/novell/httpstkd/server.pem
/etc/opt/novell/httpstkd/server.key

The following files are already modifiable by the Admin user:

The first category has names that are whatever the user names the group that they create.
/opt/novell/nrm/NRMGroups/[nrm group names]
/etc/opt/novell/nrmhconfig.conf
/etc/opt/novell/nrmsvchlthcfg.conf

<table>
<thead>
<tr>
<th>Feature</th>
<th>Yes/No</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers, devices, and services are authenticated</td>
<td>Yes</td>
<td>When gathering information with group operations, Novell Remote Manager authenticates to other servers.</td>
</tr>
<tr>
<td>Access to information is controlled</td>
<td>Yes</td>
<td>Access to information is restricted to valid users who have rights to access the server through eDirectory or access rights to the local file system. The port for accessing the login dialog box must be open through a firewall if you want the server to be accessible outside the firewall. You can restrict access to specific workstations or a range of IP addresses. For more information, see &quot;Accessing Novell Remote Manager&quot; on page 22 and &quot;Changing the HTTPSTKD Configuration&quot; on page 31.</td>
</tr>
<tr>
<td>Roles are used to control access</td>
<td>No</td>
<td>Novell Remote Manager does not have role-based management.</td>
</tr>
<tr>
<td>Logging and security auditing is done</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

---

"OES 2015 SP1: Novell Remote Manager Administration Guide"
19.2 Security Characteristics

Novell Remote Manager communicates using port 8008 and 8009. Port 8008 access the Login page, then all other communications take place through secure HTTP ports 8009. These default settings can be changed using options in the `/etc/opt/novell/httpstkd.conf` file.

The HTTPS communication uses SSL encryption. It uses the server certificate by default; however, you can reconfigure this setting if desired.

You can set the SSL key cipher strength by setting the `cipher strength` command in the `/etc/opt/novell/httpstkd.conf` file. We recommend that you set the cipher strength to high, which allows only 112-bit or greater encryption. By default it is set ALL, which allows any cipher strength. For information, see Section A.9, "SSL Key Cipher Strength Command," on page 162.

By default, Novell Remote manager sets an HttpOnly cookie attribute that specifies that the cookie is not accessible through a script. This helps mitigate the risk of cross-site scripting. For information, see Section A.5, "HttpOnly Command," on page 158.

The Admin user and users with rights equivalent to user Admin have limited root user privileges that are needed to modify only the configuration files necessary for configuring NRM or any other files that NRM has been assigned rights to allow modifying. For a list of these files, see Section 19.1, "Security Features," on page 147. The user Admin or equivalent user has access according to the Linux and LUM file rights to all other files.

19.3 Security Configuration

The following table provides a summary of the options you can change to allow or limit access to the server through Novell Remote Manager.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Yes/No</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data on the wire are encrypted by default</td>
<td>Yes</td>
<td>The following data are encrypted on the wire:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Administration via browser UI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- When logging in the administration is switching to the HTTPS protocol.</td>
</tr>
<tr>
<td>Data is stored encrypted</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Passwords, keys, and any other authentication</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>materials are stored encrypted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security is on by default</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Table 19-2 Options for Changing or Limiting Access to a Server Through Novell Remote Manager

<table>
<thead>
<tr>
<th>Issue/Feature</th>
<th>Recommendation</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL key cipher strength</td>
<td>High (112-bit or greater encryption)</td>
<td>Section A.9, “SSL Key Cipher Strength Command,” on page 162</td>
</tr>
<tr>
<td></td>
<td>The default setting is ALL, which allows any encryption level.</td>
<td></td>
</tr>
<tr>
<td>Issue/Feature</td>
<td>Recommendation</td>
<td>For More Information</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>Let the root user access Novell Remote Manager with full management rights.</td>
<td>This is the default setting. The root user is the only user with full management rights in Novell Remote Manager. By default, only the root user and LUM-enabled eDirectory users can log in to Novell Remote Manager. Non-LUM-enabled eDirectory users cannot access the server through Novell Remote Manager. We recommend that the root user be the only local user created on the system. However, if local users log in to Novell Remote Manager, their access is limited to viewing the file systems that they have the local rights to see. The management features are not available to non-root local users.</td>
<td>&quot;Accessing Novell Remote Manager&quot; on page 22.</td>
</tr>
<tr>
<td>Let all LUM-enabled eDirectory users access file system information in Novell Remote Manager.</td>
<td>All non-local user access is controlled by eDirectory and LUM. LUM-enabled eDirectory users can log in and view the file systems that they have the eDirectory rights and file system rights to see. These users (including Admin users and Admin-equivalent users) do not have management rights in Novell Remote Manager.</td>
<td>&quot;Accessing Novell Remote Manager&quot; on page 22.</td>
</tr>
<tr>
<td>Deny access to all non-LUM-enabled eDirectory users.</td>
<td>The eDirectory users that are not LUM enabled cannot access the server through Novell Remote Manager.</td>
<td></td>
</tr>
</tbody>
</table>
| Deny access to all LUM-enabled eDirectory users, including the Admin user and Admin-equivalent users. | Set the nolum option in the `/etc/opt/novell/httpstkd.conf` file and edit the `/etc/pam.d/httpstkd` file. Remove these lines: `auth sufficient pam_nam.so account sufficient pam_nam.so password sufficient pam_nam.so session optional pam_nam.so` When the nolum option is set, no LUM-enabled eDirectory user can access the server via Novell Remote Manager, including the Admin user and Admin-equivalent user. By default, non-LUM-enabled eDirectory users continue to be denied access. Only the root user has full management access to Novell Remote Manager. | • "Changing the HTTPSTKD Configuration" on page 31.  
• "Accessing and Editing the HTTPSTKD Configuration File" on page 33. |

<table>
<thead>
<tr>
<th>Issue/Feature</th>
<th>Recommendation</th>
<th>For More Information</th>
</tr>
</thead>
</table>
19.4 Nagios Security Configuration

By default, Nagios defines a default user *nagiosadmin* with no password and a default contact *nagiosadmin*. Before you can log in to the Nagios website, you must set a password for the Nagios user *nagiosadmin*. For information about configuring a password and setting up contact information for the Nagios user *nagiosadmin*, see Section 8.5.1, "Configuring Nagios Authenticated Users and Contacts," on page 47.
A.1 Address and Port Commands

Purpose

Specifies each address and port that HTTPSTKD opens and listens on.
Optionally, you can enable SSL on the port using the `keyfile` and `certfile` parameters. SSL encrypts the login, so that passwords are not sent over the Internet in plain text.

**Syntax**

```
addr ip_address:port_number

addr ip_address:port_number keyfile:key_file_path/keyfile_name.key
certfile:certificate_file_path/cerfile_name.pem
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Use</th>
</tr>
</thead>
</table>
| IP_address              | One of the following:
|                         | * 0.0.0.0                                                           |
|                         | * The assigned static IP address of the node                        |
| A DNS name is not allowed. |
| port                    | One of the following for public or secure:
|                         | * 8008 is the default public port                                   |
|                         | * 8009 is the default secure port                                   |
|                         | * any port not in use on the server                                 |
|                         | If you are accessing Novell Remote Manager outside a firewall, these ports must be open. |
| keyfile=<keyfile_path/keyfile_name.key> | A .key file is the private key used to encrypt SSL-enabled requests. The key corresponds to the public key in the certificate. |
|                         | /etc/opt/novell/httpstkd/server.key is the default path and file name on a new server installation. |
| certfile=<certificate_path/certificate_name.pem> | A .pem file is a base64 ASCII encoded SSL certificate and its public key. |
|                         | /etc/opt/novell/httpstkd/server.pem is the default path and file name on a new server installation. |

**Examples**

```
addr 0.0.0.0:8008
addr 0.0.0.0:8009 keyfile=/etc/opt/novell/httpstkd/server.key certfile=/etc/opt/novell/httpstkd/server.pem
```

**A.2 Disable Auto LUM Command**

**Purpose**

Only the root user has full management rights in Novell Remote Manager. The root user is a local superuser, and is not an eDirectory user. This allows the server to be managed even if the eDirectory authentication service is down.
Auto LUM lets eDirectory users that are enabled with Linux User Management (LUM) log in to Novell Remote Manager by using their eDirectory user names and passwords. For example, you can log in as user Admin or as a user with rights equivalent to Admin rather than logging in as user root. When LUM-enabled eDirectory users access Novell Remote Manager, they are allowed to view only the file systems that they have the eDirectory rights and file system rights to see.

**NOTE:** You can use the `supervisoronly` option to restrict access for LUM-enabled eDirectory users to only the Admin user and users with rights equivalent to the Admin user.

By default, the eDirectory users that are not LUM-enabled cannot access the server with Novell Remote Manager. They can view their files via NCP, CIFS, or AFP.

We recommend against creating local users other than the root user. However, if non-root local users access Novell Remote Manager, they must log in using the user name and password created on the local system. Only limited functionality is available. They can view only those file systems that they have the local access rights to see. The `nolum` option does not prevent the local-only users from logging in to Novell Remote Manager.

Use the `nolum` command to deny access to all LUM-enabled eDirectory users. By default, non-LUM-enabled eDirectory users continue to be denied access. Only the root user has full management access to Novell Remote Manager.

### Syntax

```
nolum
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>no setting</td>
<td>This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>To perform all management functions, users must be logged in as user root.</td>
</tr>
<tr>
<td></td>
<td>To view file system information, LUM-enabled eDirectory users can log in with their eDirectory user name and password. Non-LUM-enabled eDirectory users are denied access.</td>
</tr>
<tr>
<td></td>
<td>To view local file system information only, non-root local users can log in with their locally created user names and passwords. We recommend against creating non-root local users.</td>
</tr>
<tr>
<td></td>
<td>When the <code>nolum</code> command is not specified, HTTPSTKD checks its PAM configuration file at load time and adds the LUM configuration to it if LUM is installed but not already in its configuration.</td>
</tr>
</tbody>
</table>
A.3 Email Notification Commands (OES 11 SP1 and Earlier)

Availability

The httpstkd email notification commands are integrated with the Novell Remote Manager Health Monitor in OES 11 SP1 and earlier. The commands are not available in the HTTPSTKD configuration file beginning in OES 11 SP2, OES 2015 or later releases.

**IMPORTANT:** The Novell Remote Manager email notification system is not available in OES 2015 or later. For OES 11 SP2, OES 2015 or later, the email notification commands in the HTTPSTKD configuration file (/etc/opt/novell/httpstkd.conf) are obsoleted by the alert notification system for Nagios. After you install or upgrade to OES 11 SP2, OES 2015 or later, you must configure Nagios and set up an email address for the nagiosadmin user. You can also define other Nagios contacts. You can set up various notification methods for each Nagios contact, and assign the contacts to receive notifications for designated monitored service. For more information, see Section 8.5, “Configuring Nagios,” on page 47 Section 8.9, “Modifying the Nagios Notification Methods for Contacts,” on page 58.

**Purpose**

Sets up email notification service in Novell Remote Manager.

You can specify up to two mail servers and up to eight recipients to receive email when a notification is specified in the Novell Remote Manager server health area. Use a separate command line for each server or email address.
Syntax

mailserver IP_address
mailto email_address

<table>
<thead>
<tr>
<th>Command</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>no setting</td>
<td>Email notification is not configured. This is the default setting.</td>
</tr>
<tr>
<td>mailserver</td>
<td>Sends email notification to the specified mail server. You can specify up to two mail servers.</td>
</tr>
<tr>
<td>mailto</td>
<td>Sends email notification to the specified user. You can specify up to eight users.</td>
</tr>
</tbody>
</table>

Example

The following commands send email notifications to mail servers mail.bobs1bank.com and smtp.bobs1bank.com:

mailserver mail.bobs1bank.com
mailserver smtp.bobs1bank.com

The following commands send email notifications to users Bob, George, and Mary from the mail server bobs1bank.com:

mailto bob@bobs1bank.com
mailto george@bobs1bank.com
mailto mary@bobs1bank.com

A.4 Filtering Commands

Purpose

Blocks access to Novell Remote Manager from all addresses except those specified by these filteraddr and filtersubnet commands.

Syntax

filteraddr IP_address
filtersubnet IP_address subnet_mask

<table>
<thead>
<tr>
<th>Command</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>not specified</td>
<td>Allows access from any address. This is the default setting.</td>
</tr>
<tr>
<td>filteraddr</td>
<td>Allows access from specific addresses only.</td>
</tr>
<tr>
<td>filtersubnet</td>
<td>Allows access from any address on the specified network or subnet.</td>
</tr>
</tbody>
</table>

Examples

The following command allows access only from address 192.168.20.1:

filteraddr 192.168.20.1

The following command allows access from only addresses 192.56.56.0 through 192.56.59.255:
A.5 **HttpOnly Command**

**Purpose**

Novell Remote manager sets an HttpOnly cookie attribute that specifies that the cookie is not accessible through a script. This helps mitigate the risk of cross-site scripting.

**Syntax**

If the HttpOnly flag is included in the HTTP response header, the cookie cannot be accessed through a client side script.

If you modify the setting, you must restart Novell Remote Manager.

`HttpOnly <true|false>`

<table>
<thead>
<tr>
<th>Option</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>Include HttpOnly as an attribute in the response header. This is the default setting.</td>
</tr>
<tr>
<td>false</td>
<td>Do not include HttpOnly in the response header.</td>
</tr>
</tbody>
</table>

To disable the HttpOnly attribute:

1. Log in to the server as the `root` user, then open a terminal console.
2. Stop the `httpstkd` daemon by entering
   
   ```
   rcnovell-httpstkd stop
   ```
3. Open the `/etc/opt/novell/httpstkd.conf` file in a text editor.
4. Review the potential security concerns for changing HttpOnly to false.
5. Change the setting from
   
   ```
   HttpOnly true
   ```
   
   to
   
   ```
   HttpOnly false
   ```
6. Save the file and exit the text editor.
7. Start the `httpstkd` daemon by entering
   
   ```
   rcnovell-httpstkd start
   ```

**Examples**

- `HttpOnly true`
- `HttpOnly false`
A.6 InventoryResolveNonLumOwnerName Command

Purpose

The `InventoryResolveNonLumOwnerName` command is used when you perform an inventory of NSS volumes and the file owner UID is set to the Nobody user. The Nobody user is reported when a file is owned by a Novell eDirectory user that is not enabled with Linux User Management (LUM).

Syntax

If you modify the setting, you must restart Novell Remote Manager.

```
InventoryResolveNonLumOwnerName <false|true>
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>The inventory does not resolve the user IDs of non-LUM-enabled file owners. The owner is reported as the Nobody user. This is the default setting. This provides faster performance for an inventory of files on an NSS volume when eDirectory users are not LUM enabled.</td>
</tr>
<tr>
<td>true</td>
<td>The inventory tries to resolve the user IDs of non-LUM-enabled file owners by using NSS APIs. This can result in a major performance impact for the inventory. The more non-LUM-enabled file owners the inventory encounters, the longer it takes to complete the inventory.</td>
</tr>
</tbody>
</table>

Examples

The following example does not resolve the user IDs of file owners that are not LUM enabled. This is the default setting. The non-LUM-enabled owners are reported as the Nobody user.

```
InventoryResolveNonLumOwnerName false
```

The following example resolves the user IDs of file owners that are not LUM enabled to the user name. The more non-LUM-enabled owners encountered, the longer the inventory can take.

```
InventoryResolveNonLumOwnerName true
```

A.7 Language Commands

Purpose

Sets up a mapping of HTTP Accept-Language header tags for Linux locales. These locales determine the languages in which the browser can view content through the Novell Remote Manager utility.

To see a list of possible locales on your Linux server, enter the following at a shell prompt:

```
locale -a
```

Syntax

```
lang HTTP_language_string locale_string
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>lang</td>
<td>Use the following settings:</td>
</tr>
<tr>
<td></td>
<td>• English: en en_US.UTF8</td>
</tr>
<tr>
<td></td>
<td>• US English: en-us en_US.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Chinese Simplified: zh-cn zh_CN.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Chinese Traditional: zh-tw zh_TW.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Czech: cs cs_CZ.UTF8</td>
</tr>
<tr>
<td></td>
<td>• French: fr fr_FR.UTF</td>
</tr>
<tr>
<td></td>
<td>• German: de de_DE.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Hungarian: hu hu_HU.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Italian: it it_IT.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Japanese: ja ja_JP.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Polish: pl pl_PL.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Portuguese-Brazil: pt pt_BR.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Russian: ru ru_RU.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Spanish: es es_ES.UTF8</td>
</tr>
<tr>
<td></td>
<td>• Slovak: sk sk_SK.UTF8</td>
</tr>
</tbody>
</table>

These are the default settings for this release.

In this release, Novell Remote Manager supports English, Chinese Simplified, Chinese Traditional, Czech, French, German, Hungarian, Italian, Japanese, Polish, Portuguese-Brazil, Russian, Spanish, and Slovak.
Example

The following commands set the browser languages for English, French, Japanese, and Portuguese:

```plaintext
lang en     en_US.UTF8
lang en-us  en_US.UTF8
lang zh-cn  zh_CN.UTF8
lang zh-tw  zh_TW.UTF8
lang cs     cs_CZ.UTF8
lang cs-cz  cs_CZ.UTF8
lang fr     fr_FR.UTF8
lang fr-fr  fr_FR.UTF8
lang de     de_DE.UTF8
lang de-de  de_DE.UTF8
lang hu     hu_HU.UTF8
lang hu-hu  hu_HU.UTF8
lang it     it_IT.UTF8
lang it-it  it_IT.UTF8
lang ja     ja_JP.UTF8
lang ja-jp  ja_JP.UTF8
lang pl     pl_PL.UTF8
lang pl-pl  pl_PL.UTF8
lang pt     pt_BR.UTF8
lang pt-BR  pt_BR.UTF8
lang ru     ru_RU.UTF8
lang ru-ru  ru_RU.UTF8
lang es     es_ES.UTF8
lang es-es  es_ES.UTF8
lang sk     sk_SK.UTF8
lang sk-sk  sk_SK.UTF8
```

More Information

If you are upgrading this server and you want to use this option, you need to add these parameters to the `/etc/opt/novell/httpstkd.conf` file for this server.

### A.8 Load Command

#### Purpose

Loads plug-in files used by Novell Remote Manager.

#### Syntax

```plaintext
load plug-in_file_path/name
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>plug-in_file_path</strong></td>
<td><code>/opt/novell/lib/</code> is the default path for Novell Remote Manager plug-in files.</td>
</tr>
<tr>
<td><strong>plug-in_file_name</strong></td>
<td><code>libnrm.so</code> is a default plug-in for Novell Remote Manager.</td>
</tr>
</tbody>
</table>

#### Examples

```plaintext
load nrm.so
load /opt/novell/lib/libnrm.so
```
A.9 SSL Key Cipher Strength Command

Purpose

The Cipher command sets the bit strength for the SSL key that is required to access Novell Remote Manager. If you modify the setting, you must restart NRM.

Syntax

cipher strength

<table>
<thead>
<tr>
<th>Option</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Allows any negotiated encryption level. This is the default setting.</td>
</tr>
<tr>
<td>low</td>
<td>Allows less than 56-bit encryption.</td>
</tr>
<tr>
<td>medium</td>
<td>Allows 56-bit up to 112-bit encryption.</td>
</tr>
<tr>
<td>high</td>
<td>Allows 112-bit or greater encryption</td>
</tr>
</tbody>
</table>

Example

The following example allows access to Novell Remote Manager only with encryption that is 112-bit or greater:

cipher high

You must restart Novell Remote Manager to apply the change.

A.10 Supervisor Only Command

Purpose

Disables access to the server through Novell Remote Manager for all users except root. If Linux User Management is enabled for Novell Remote Manager, eDirectory user Admin and eDirectory users with rights equivalent to user Admin also have access to the server through Novell Remote Manager and can perform the same tasks as user root.

Syntax

supervisoronly

<table>
<thead>
<tr>
<th>Option</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>no setting</td>
<td>This is the default setting.</td>
</tr>
</tbody>
</table>

Local users and all LUM-enabled eDirectory users can log in to Novell Remote Manager.

The non-root and non-admin users have limited access to the server through Novell Remote Manager. They can access only the server’s file systems that they have rights to and can perform very limited tasks such as file upload and text search.
<table>
<thead>
<tr>
<th>Option</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>supervisoronly</td>
<td>Lets only user root and eDirectory user Admin and users with rights equivalent to Admin have access to the server through Novell Remote Manager. LUM must be set for eDirectory user access.</td>
</tr>
</tbody>
</table>

**Example**

supervisoronly

**More Information**

If you are upgrading this server and you want to use this option, you need to add these parameters to the /etc/opt/novell/httpstkd.conf file for this server.
Novell Remote Manager Packages

Table B-1 lists the packages that are installed when the Novell Remote Manage pattern is installed on an Novell Open Enterprise Server (OES) 2015 SP1 server.

**Table B-1 Packages Contained in the Novell Remote Manager Pattern**

<table>
<thead>
<tr>
<th>Package (RPM)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>novell-lum-providers</td>
<td>A set of CIM providers to facilitate the management of Linux User Management, which is a plug-in to PAM.</td>
</tr>
<tr>
<td>novell-nrm</td>
<td>Novell Remote Manager, web-based Linux machine management, and control interface. It contains all the binaries and necessary components for Novell Remote Manager.</td>
</tr>
</tbody>
</table>

Table B-2 lists the plug-in software that adds functionality to Novell Remote Manager when the related OES Services pattern is installed:

**Table B-2 Packages for Program Plug-Ins to Novell Remote Manager**

<table>
<thead>
<tr>
<th>RPM</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>novell-ncpserv-nrm</td>
<td>NRM plug-in for the Novell NCP Server and Dynamic Storage Technology</td>
</tr>
<tr>
<td>novell-cifs-nrm</td>
<td>NRM plug-in for Novell CIFS Services</td>
</tr>
<tr>
<td>novell-afp-nrm</td>
<td>NRM plug-in for Novell AFP Services</td>
</tr>
</tbody>
</table>

Table B-3 lists the software that Novell Remote Manager depends on to report server and services health information in OES 2015 SP1:

**Table B-3 Open Source Packages Used for Server and Services Health Monitoring in OES 2015 SP1**

<table>
<thead>
<tr>
<th>RPM</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>novell-ganglia-monitor-core-gmetad</td>
<td>Ganglia Meta daemon that gathers the health statistics about the server</td>
</tr>
<tr>
<td>novell-ganglia-monitor-core-gmond</td>
<td>Ganglia Monitor daemon that provides the Ganglia monitoring service</td>
</tr>
<tr>
<td>novell-ganglia-web</td>
<td>Ganglia Distributed Monitoring System that provides historical graphs of the collected system metrics</td>
</tr>
<tr>
<td>nagios</td>
<td>Core programs for the Nagios Network Monitor</td>
</tr>
<tr>
<td>nagios-plugins</td>
<td>Nagios Plug-Ins that perform the service checks and return the status to Nagios</td>
</tr>
<tr>
<td>nagios-www</td>
<td>The HTML and CGI files for the Nagios web interface</td>
</tr>
</tbody>
</table>
Table B-4 lists the software that Novell Remote Manager depends on to report system health information in OES 11 SP1 and earlier:

**Table B-4  Key Dependencies of the Novell Remote Manager Pattern in OES 11 SP1 and Earlier**

<table>
<thead>
<tr>
<th>RPM</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sblim-sfcb</td>
<td>The Small Footprint CIM Broker (sfcb) is a CIM server that conforms to the CIM Operations over HTTP protocol. It supports providers written against the Common Manageability Programming Interface (CMPI)</td>
</tr>
<tr>
<td>novell-hms-providers</td>
<td>A set of CIM providers that facilitate the gathering of data for Health Management Services (HMS)</td>
</tr>
</tbody>
</table>