

Novell Remote Manager Administration Guide

Open Enterprise Server 11 SP2

January 2014

Novell.

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2004–2014 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

This product includes materials licensed under the Apache license, including Apache and Tomcat.

Contents

About This Guide	9
1 Overview of Novell Remote Manager for Linux	11
1.1 Benefits of Using Novell Remote Manager	11
1.2 Other Management Utilities	12
1.3 What's Next	12
2 What's New or Changed in Novell Remote Manager	15
2.1 What's New (OES 11 SP2)	15
2.2 What's New (OES 11 SP1)	17
2.3 What's New (OES 11)	17
3 Migrating Novell Remote Manager from NetWare to OES 11	21
3.1 Coexistence	21
3.1.1 Compatibility	21
3.1.2 Coexistence Issues	21
3.2 Migration	21
4 Managing a Virtualized Linux Server with Novell Remote Manager	23
5 Installing Novell Remote Manager for Linux	25
5.1 Installing Novell Remote Manager During the Initial Server Installation	25
5.2 Installing Novell Remote Manager After the Initial Server Installation	25
6 Accessing Novell Remote Manager for Linux	27
6.1 System Requirements	27
6.2 Accessing Novell Remote Manager	28
6.3 Starting or Stopping HTTPSTKD	30
6.4 Understanding the Layout of Novell Remote Manager	30
6.4.1 Header Frame	33
6.4.2 Overall Health Indicator	33
6.4.3 Navigation Frame	34
6.4.4 Program Plug-Ins in the Navigation Frame	35
6.4.5 Main Content Frame	35
6.4.6 Online Help	36
6.5 Accessing Configuration Options	36
6.6 Accessing Online Help	36
6.7 Accessing Novell Web Pages	36
7 Changing the HTTPSTKD Configuration	37
7.1 Accessing and Editing the HTTPSTKD Configuration File	39
7.2 Accessing and Editing the HTTPSTKD PAM Configuration File	40
7.3 Restarting the HTTPSTKD Daemon	41

7.4	Viewing the HTTP Logs	41
7.5	Viewing and Creating Certificates for Novell Remote Manager	41
7.6	Extending the eDirectory Schema for Novell Remote Manager Group Operations	42
8	Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2)	45
8.1	Monitoring Server Health	46
8.1.1	Viewing the Overall Server Health Status	46
8.1.2	Setting the Health Status Refresh Rate	46
8.2	Configuring Ganglia	47
8.2.1	Ganglia Requirements	47
8.2.2	Configuring Ganglia gmond in Multicast Mode or Unicast Mode	48
8.3	Stopping and Starting Ganglia gmond and gmetad	50
8.4	Monitoring Server Health with Ganglia	50
8.5	Configuring Nagios	53
8.5.1	Configuring Nagios Authenticated Users and Contacts	53
8.5.2	Configuring Nagios Monitoring	57
8.5.3	Accessing the Nagios Website	59
8.5.4	Using Nagios Plug-Ins	59
8.5.5	Using Object Configuration Files	60
8.5.6	Additional Information	60
8.6	Monitoring Service Health with Nagios	60
8.7	Restarting Nagios	61
8.8	Managing Nagios Users	61
8.8.1	Creating or Re-Creating a Nagios User	62
8.8.2	Setting Passwords for Nagios Users	62
8.8.3	Deleting a Nagios User	62
8.8.4	Configuring Nagios Contacts and Notification Methods for Them	63
8.8.5	Configuring Nagios CGI Authorization for Contacts	63
8.9	Modifying the Nagios Notification Methods for Contacts	64
8.10	Configuring Nagios Logging	64
8.11	Viewing the PIDs or Monitoring the Health of Processes	66
8.12	Monitoring or Killing an Individual Process	67
8.13	Troubleshooting a Suspect or Bad Health Status	68
9	Diagnosing Problems Using Health Monitor (OES 11 SP1)	69
9.1	Monitoring Server Health	69
9.1.1	Accessing the Health Monitor	69
9.1.2	Viewing the Health Monitor	70
9.1.3	Monitoring Overall Server Health or the Health of a Specific Item	70
9.1.4	Configuring the Items to Monitor	73
9.1.5	Configuring Email Notification for Server Health Status	74
9.2	Viewing the PIDs or Monitoring the Health of Processes	74
9.3	Monitoring or Killing an Individual Process	75
9.4	Troubleshooting a Suspect or Bad Health Status	75
10	Viewing File Systems	77
10.1	Viewing Mounted Devices and Performing Actions on Them	78
10.2	Browsing File Systems and Performing Actions on Them	79
10.2.1	Viewing or Changing File or Directory Attributes	80
10.2.2	Viewing Details about Directories and Performing Actions on Them	81
10.2.3	Uploading a File to the Server	81
10.2.4	Downloading a File from the Server to a Local Workstation	82
10.2.5	Searching for Text in Files	82

10.2.6	Viewing the Details of a File and Performing Specific Actions	82
10.2.7	Viewing Individual Files	83
10.3	Viewing Partition Information	83
11	Managing Linux	85
11.1	Accessing VNC Consoles	85
11.2	Viewing Kernel Modules	88
11.3	Viewing Memory Information	88
11.4	Shutting Down and Restarting the Host	90
11.5	Managing Packages	90
11.6	Managing Processes	92
11.7	Scheduling cron Jobs to Run on the Server	94
12	Managing Hardware	97
12.1	Viewing Processors	97
12.2	Viewing Interrupt Information	98
12.3	Viewing I/O Memory Information	99
12.4	Viewing I/O Port Information	100
12.5	Viewing SMBIOS Information	101
13	Using Group Operations	103
13.1	Building and Configuring a Monitoring Group	104
13.2	Saving a Group	108
13.2.1	Saving the Group to the Local Server	108
13.2.2	Saving the Group and Associating It with an eDirectory Object	109
13.3	Accessing an Existing Group	109
13.4	Changing an Existing Group	109
13.5	Deleting an Existing Group	110
13.6	Generating and Viewing Server Reports	110
13.6.1	Compare Server Up Time Report	110
13.7	Viewing Monitored Items	111
13.8	Viewing Group Monitoring Types	112
13.9	Defining or Editing Group Monitoring Types	113
13.10	Discovering Items on the Network to Monitor	114
14	Managing NCP Services	117
14.1	Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux	119
14.1.1	NCP Volumes (NCP Shares)	119
14.1.2	NCP Server Parameters	120
14.1.3	NCP Server Connections	120
14.1.4	NCP Trustee Reports	121
14.1.5	NCP Logs and Audit Logs	121
14.1.6	NCP Server Statistics	122
14.1.7	NCP Server Diagnostics	122
14.1.8	Dynamic Storage Technology	123
14.2	Browsing NSS Volumes and Performing Actions on Them	124
14.2.1	Viewing Information about an NSS Volume	124
14.2.2	Viewing the Linux POSIX Details of an NSS Directory and Performing Specific Actions on It	126
14.2.3	Viewing the Linux POSIX Details of a File and Performing Specific Actions on It	127
14.2.4	Browsing an NSS Volume and Setting Rights and File System Attributes on Directories and Files	128

14.2.5	Salvaging and Purging Deleted Files on an NSS Volume	132
14.2.6	Purging a Deleted NSS Volume	132
14.2.7	Viewing Open File Information for an NSS Volume	133
14.3	Generating Inventories for Directories or NCP Volumes	133
14.3.1	Generating a File Inventory Report	134
14.3.2	Generating an NCP Volume Inventory Report	135
14.3.3	Viewing a Saved NCP Inventory Report	137
14.3.4	Emailing a Saved NCP Inventory Report (OES 11 SP1)	137
14.4	Generating a Custom Inventory Report from a File Inventory Report	138
14.5	Performing Actions on Files from Custom Reports	139
14.5.1	Moving Selected Files	139
14.5.2	Copying Selected Files	140
14.5.3	Deleting Selected Files	140
14.5.4	Opening or Downloading a File	140
14.5.5	Managing Individual Files	140
14.6	Generating and Viewing NCP Trustee Reports for NSS Volumes	140
14.6.1	Generating an NCP Trustee Report	141
14.6.2	Viewing a Saved NCP Trustee Report	141
14.6.3	Emailing a Saved NCP Trustee Report (OES 11 SP1)	141
15	Managing Dynamic Storage Technology Options	143
16	Managing CIFS Services	147
16.1	Managing CIFS Connections	148
16.2	Viewing Log Information	148
16.3	Managing Open Files	149
17	Managing AFP Services	151
17.1	Managing AFP Connections	152
17.2	Viewing Log Information	152
17.3	Managing Open Files	153
18	Tasks Quick Reference	155
19	Troubleshooting Novell Remote Manager	159
19.1	Daemon httpstkd Is Unable to Start	159
19.2	Error while loading shared libraries: libldapx.so.0	159
19.3	Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 11 SP2	160
19.4	Inventory Graphics Are Not Displayed in the Web Browser	161
19.5	Ganglia Statistical Graphics Are Not Displayed in the Web Browser	165
19.5.1	Firefox	165
19.5.2	Internet Explorer	166
19.5.3	Chrome	166
20	Security Considerations	167
20.1	Security Features	167
20.2	Security Characteristics	169
20.3	Security Configuration	170
20.4	Nagios Security Configuration	172

A	HTTPSTKD Configuration File Options	173
A.1	Address and Port Commands	174
A.2	Disable Auto LUM Command	175
A.3	Email Notification Commands (OES 11 SP1 and Earlier)	176
A.4	Filtering Commands	177
A.5	HttpOnly Command	178
A.6	InventoryResolveNonLumOwnerName Command	179
A.7	Language Commands	179
A.8	Load Command	181
A.9	SSL Key Cipher Strength Command	182
A.10	Supervisor Only Command	182
B	Novell Remote Manager Packages	185
C	Documentation Updates	187
C.1	January 2014 (OES 11 SP2)	187
C.1.1	Accessing Novell Remote Manager for Linux	188
C.1.2	Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2)	189
C.1.3	Diagnosing Problems Using Health Monitor (OES 11 SP1)	189
C.1.4	HTTPSTKD Configuration File Options	189
C.1.5	Managing AFP Services	189
C.1.6	Managing CIFS Services	190
C.1.7	Managing Dynamic Storage Technology Options	190
C.1.8	Managing NCP Services	190
C.1.9	Novell Remote Manager Packages	190
C.1.10	Overview of Novell Remote Manager for Linux	190
C.1.11	Security Considerations	191
C.1.12	Troubleshooting Novell Remote Manager	191
C.1.13	Using Group Operations	191
C.1.14	Viewing File Systems	191
C.1.15	What's New or Changed in Novell Remote Manager	192
C.2	August 2012 (OES 11 SP1)	192
C.2.1	Managing a Virtualized Linux Server with Novell Remote Manager	192
C.2.2	Viewing File Systems	192
C.2.3	What's New or Changed in Novell Remote Manager	192

About This Guide

This guide describes how to access and use Novell Remote Manager on a host that is running Novell Open Enterprise Server (OES) 11 SP1 on the SUSE Linux Enterprise Server (SLES) 11 Service Pack 2 (SP2) operating system. This guide includes the following information:

- ♦ Chapter 1, “Overview of Novell Remote Manager for Linux,” on page 11
- ♦ Chapter 2, “What’s New or Changed in Novell Remote Manager,” on page 15
- ♦ Chapter 3, “Migrating Novell Remote Manager from NetWare to OES 11,” on page 21
- ♦ Chapter 4, “Managing a Virtualized Linux Server with Novell Remote Manager,” on page 23
- ♦ Chapter 5, “Installing Novell Remote Manager for Linux,” on page 25
- ♦ Chapter 6, “Accessing Novell Remote Manager for Linux,” on page 27
- ♦ Chapter 7, “Changing the HTTPSTKD Configuration,” on page 37
- ♦ Chapter 8, “Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2),” on page 45
- ♦ Chapter 9, “Diagnosing Problems Using Health Monitor (OES 11 SP1),” on page 69
- ♦ Chapter 10, “Viewing File Systems,” on page 77
- ♦ Chapter 11, “Managing Linux,” on page 85
- ♦ Chapter 12, “Managing Hardware,” on page 97
- ♦ Chapter 13, “Using Group Operations,” on page 103
- ♦ Chapter 14, “Managing NCP Services,” on page 117
- ♦ Chapter 15, “Managing Dynamic Storage Technology Options,” on page 143
- ♦ Chapter 16, “Managing CIFS Services,” on page 147
- ♦ Chapter 17, “Managing AFP Services,” on page 151
- ♦ Chapter 18, “Tasks Quick Reference,” on page 155
- ♦ Chapter 19, “Troubleshooting Novell Remote Manager,” on page 159
- ♦ Chapter 20, “Security Considerations,” on page 167
- ♦ Appendix A, “HTTPSTKD Configuration File Options,” on page 173
- ♦ Appendix B, “Novell Remote Manager Packages,” on page 185
- ♦ Appendix C, “Documentation Updates,” on page 187

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 \(http://www.novell.com/documentation/feedback.html\)](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 11 SP2 documentation website \(http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html\)](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Additional Documentation

For information about other OES 11 SP2 services and file systems, see the [OES 11 SP2 documentation website \(http://www.novell.com/documentation/oes11/\)](http://www.novell.com/documentation/oes11/).

1 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 11](#)
- ♦ [Section 1.2, "Other Management Utilities," on page 12](#)
- ♦ [Section 1.3, "What's Next," on page 12](#)

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 11. For an understanding of which utilities are best for the task you need to perform, see “[OES Utilities and Tools](#)” in the *OES 11 SP2: 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*

For Information About	See
Accessing and understanding the layout of Novell Remote Manager	Chapter 6, “Accessing Novell Remote Manager for Linux,” on page 27
Determining whether Novell Remote Manager for Linux is compatible with other operating systems and how it fits in your current network	Chapter 3, “Migrating Novell Remote Manager from NetWare to OES 11,” on page 21
Managing a virtualized OES 11 server with Novell Remote Manager.	Chapter 4, “Managing a Virtualized Linux Server with Novell Remote Manager,” on page 23
Installing Novell Remote Manager for Linux	Chapter 5, “Installing Novell Remote Manager for Linux,” on page 25
Changing the configuration of Novell Remote Manager	Chapter 7, “Changing the HTTPSTKD Configuration,” on page 37

For Information About	See
Using Novell Remote Manager to monitor and manage your OES servers	<ul style="list-style-type: none"> ♦ Chapter 8, “Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2),” on page 45 ♦ Chapter 9, “Diagnosing Problems Using Health Monitor (OES 11 SP1),” on page 69 ♦ Chapter 10, “Viewing File Systems,” on page 77 ♦ Chapter 11, “Managing Linux,” on page 85 ♦ Chapter 12, “Managing Hardware,” on page 97 ♦ Chapter 13, “Using Group Operations,” on page 103
Things to consider for setting up your system in a secure environment.	Chapter 20, “Security Considerations,” on page 167

Table 1-2 *Information about Plug-Ins to Novell Remote Manager*

For Information About	See
Dynamic Storage Technology	<ul style="list-style-type: none"> ♦ Chapter 14, “Managing NCP Services,” on page 117 ♦ OES 11 SP2: Dynamic Storage Technology Administration Guide
NCP Server	<ul style="list-style-type: none"> ♦ Chapter 14, “Managing NCP Services,” on page 117 ♦ OES 11 SP2: NCP Server for Linux Administration Guide
Novell AFP (in OES 11 SP2 and later)	<ul style="list-style-type: none"> ♦ Chapter 17, “Managing AFP Services,” on page 151 ♦ OES 11 SP2: Novell AFP for Linux Administration Guide
Novell CIFS (in OES 11 SP2 and later)	<ul style="list-style-type: none"> ♦ Chapter 16, “Managing CIFS Services,” on page 147 ♦ OES 11 SP2: Novell CIFS for Linux Administration Guide

2 What's New or Changed in Novell Remote Manager

This section describes the changes made to Novell Remote Manager since the Novell Open Enterprise Server (OES) 11 release.

- [Section 2.1, “What’s New \(OES 11 SP2\),” on page 15](#)
- [Section 2.2, “What’s New \(OES 11 SP1\),” on page 17](#)
- [Section 2.3, “What’s New \(OES 11\),” on page 17](#)

2.1 What's New (OES 11 SP2)

Novell Remote Manager provides the following enhancements and changes in OES 11 SP2:

Managing AFP Services

The AFP plug-in for Novell Remote Manager allows you to manage AFP connections and open files for Novell AFP users. For an overview of the AFP plug-in, see [“Managing AFP Services” \(http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nrm_afp.html\)](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nrm_afp.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Managing CIFS Services

The CIFS plug-in for Novell Remote Manager allows you to manage CIFS connections and open files for Novell CIFS users. For an overview of the CIFS plug-in, see [“Managing CIFS Services” \(http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nrm_cifs.html\)](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nrm_cifs.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Ganglia and Nagios Health Monitoring Tools

Ganglia and Nagios open source health monitoring tools replace the Health Monitor function in Novell Remote Manager in OES 11 SP2. Unlike the Health Monitor, Ganglia and Nagios tools do not use SFCB for management communications. See [“Diagnosing Problems Using Ganglia and Nagios \(OES 11 SP2\)” \(http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_ganglia_nagios.html\)](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_ganglia_nagios.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Ganglia and Nagios Monitoring Tools Obsolete the NRM Health Monitor

The Health Monitor function in Novell Remote Manager is obsoleted in OES 11 SP2. It is replaced by the Ganglia and Nagios open source monitoring tools, which do not use the Small Footprint CIM Broker (SFCB) for communications. For information about configuring and using Ganglia and Nagios to monitor the health of the server and services, see “[Diagnosing Problems Using Ganglia and Nagios](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_ganglia_nagios.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_ganglia_nagios.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

For information about using the Health Monitor in OES 11 SP1 and earlier releases, see “[Diagnosing Problems Using Health Monitor \(OES 11 SP1\)](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_monitor_oes11sp1.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/health_monitor_oes11sp1.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Nagios Alert Notification Obsoletes HTTPSTKD Email Notification

The Novell Remote Manager email notification system is obsoleted in OES 11 SP2. For health monitoring, it is replaced by the Nagios alert notification system, which is used to send alerts from the Ganglia and Nagios health monitoring tools.

After you install or upgrade to OES 11 SP2, the Novell Remote Manager email notification system is not available. The commands `mailserver` and `mailto` are not found in the HTTPSTKD configuration file (`/etc/opt/novell/httpstk.conf`) for a new install, and they are no longer supported after an upgrade.

Other functions or plug-ins that leveraged the HTTPSTKD email notification commands do not work with the Nagios alert notification system. Thus, they do not work in OES 11 SP2. For example, the NCP Server plug-in *Manage NCP Services*, the *Send* option in the *Email Report* column no longer works on the NCP Inventory Reports page and the NCP Trustee Reports page. This issue will be addressed in a future release.

In order to receive health monitoring alerts from Ganglia and Nagios, you must configure Nagios and its alert notification system. You must set up an email address for the `nagiosadmin` user. You can 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 services. For more information, see “[Configuring Nagios](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nagios-config.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nagios-config.html) and “[Configuring Nagios Notification System for Contacts](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nagios_notifications.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nagios_notifications.html) in the *OES 11 SP2: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Support for Internet Explorer 10

Web-based access to Novell Remote Manager is supported for the Internet Explorer 10 web browser in the desktop user interface view for Windows 7 clients and Windows 8 clients.

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

Support for Safari 6.0 on Mac OS X 10.8

Web-based access to Novell Remote Manager is supported for the Apple Safari 6.0 web browser on Mac OS X 10.8 clients.

Availability for prior releases: January 2013 Scheduled Maintenance for OES 11 and OES 11 SP1

2.2 What's New (OES 11 SP1)

Novell Remote Manager supports OES 11 SP1 running on 64-bit SUSE Linux Enterprise Server (SLES) 11 SP2. In addition to bug fixes, the following enhancement is available:

NCP Server Plug-In: NCP Trustee Report

Under *Manage NCP Services*, the new *View Trustee Reports* option opens the NCP Trustee Reports page where you can generate a trustee report for a specified NSS volume. You can display the last trustee report in the web browser, or send the report to the email addresses that you have preconfigured for Novell Remote Manager. The trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume. For information, see [“Generating and Viewing NCP Trustee Reports for NSS Volumes”](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/trustee_reports.html) (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/trustee_reports.html) in the *OES 11 SP1: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

2.3 What's New (OES 11)

Novell Remote Manager has been modified to run on Novell Open Enterprise Server 11. In addition to bug fixes, the following changes and enhancements are available:

HttpOnly Command

The HttpOnly configuration option is available in the Novell Remote Manager `/etc/opt/novell/httpstkd.conf` file. 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 [“HttpOnly Command”](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/httponly.html) (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/httponly.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

InventoryResolveNonLumOwnerName Command

The `InventoryResolveNonLumOwnerName` configuration option is available in the Novell Remote Manager `/etc/opt/novell/httpstkd.conf` file. This allows you to choose whether the inventory of a Novell Storage Services (NSS) volume reports the names of owners as the Nobody user if their eDirectory usernames are not enabled with Linux User Management. By default, this option is set to false (not resolved) in order to give you faster performance for an inventory of files on an NSS volume. For information, see [“InventoryResolveNonLumOwnerName Command”](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/bwv2pua.html) (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/bwv2pua.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

SSL Key Cipher Strength Command

You can set the cipher strength for the SSL key in the `/etc/opt/novell/httpstkd.conf` file. The default allows any encryption level. A setting of High is recommended. For information, see [“SSL Key Cipher Strength Command”](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/budlpt0.html) (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/budlpt0.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

VNC Consoles

The root user can view VNC consoles from within Novell Remote Manager. This capability requires that the HttpOnly security feature be disabled in the `/etc/opt/novell/httpstk.conf` file. For information, see “[HttpOnly Command](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/httponly.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/httponly.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

General File Inventory

On the File System Listing page (*View File System > View File System Listing*), the *Inventory* link generates a *General File Inventory* report with statistics about the files stored on a selected file system path or sub-folder path. For information, see “[Inventorying Directories or NCP Volumes](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/b2kl4kn.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/b2kl4kn.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

NCP Volume Inventory

- ♦ The *View File Systems > NCP Volume Inventory* option allows you to view a list of NCP volumes and generate inventories for them.
- ♦ The Volume Information page (*Manage NCP Services > Manage Shares*, then click the NSS volume name link), for a volume provides an *Inventory* option to generate an inventory. This provides the same output as running *View File System > General File Inventory* for Linux paths and for *View File Systems > NCP Volume Inventory* for NCP volumes.
- ♦ An inventory report is saved when you run an inventory on an NCP volume. You can view the last saved report by going to the *Manage NCP Services > Volume Inventory Reports* page and clicking the *View Last Report > Display* option for the volume. The saved report provides the same statistics as running *View File Systems > NCP Volume Inventory*. Graphics are not available in a saved report.
- ♦ You can email a saved NCP volume inventory report to addresses that are configured in the `/etc/opt/novell/httpstk.conf` file. To send the report, go to the *Manage NCP Services > Volume Inventory Reports* page and click the *Email Report > Send* option for the volume.
- ♦ In a file inventory for NSS volumes, the *File Owner Profile* reports the eDirectory identity of the file owner without requiring the users to be enabled with Linux User Management (LUM).

For information, see “[Inventorying Directories or NCP Volumes](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/b2kl4kn.html)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/b2kl4kn.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Open Connections for NCP Volumes and NSS Volumes

On the *Connection Information* page (*Manage NCP Services > Manage Connections*, then select a connection link under *Connections*) for a selected connection, the *Open Files* list now links to the file and lock details for each file that is held open by a connection. For information, see “[Viewing Connections for NCP Server](http://www.novell.com/documentation/oes11/file_ncp_lx/data/ba47cgt.html)” (http://www.novell.com/documentation/oes11/file_ncp_lx/data/ba47cgt.html) in the *OES 11: NCP Server for Linux Administration Guide* (http://www.novell.com/documentation/oes11/file_ncp_lx/data/h9izvdye.html).

Salvage and Purge Deleted Files for NSS Volumes

On the Share Information page (*Manage NCP Services > Manage Shares*, then click the *Information* (i) icon to the left of the NSS volume name) and on the Directory Information page (*Manage NCP Services > Manage Shares*), then navigate to a directory of interest and click the *Directory Information* icon to the left of the directory name), the following capabilities were added for salvaging and purging deleted files for NSS volumes where the Salvage attribute is enabled:

- ♦ The *Salvageable Files* list option allows you to view a list of deleted files that are available for salvage or purge in the selected directory on an NSS volume.
- ♦ The *Purge* option allows you to permanently remove a deleted file from the file system.
- ♦ The *Salvage* option allows you to recover a deleted file.
- ♦ The *Purge all files* option allows you to permanently remove all deleted files on a selected volume.

For information, see “[Salvaging and Purging Deleted Files on an NSS Volume](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nssactions.html#nsssalvage)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nssactions.html#nsssalvage) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

Create, Rename, and Delete Directories

On the Directory Information page (*View File System > View File System Listing*, navigate to the directory of interest, then click the *Directory Information* icon to the left of the directory name), the following capabilities were added:

- ♦ The *Delete Directory and Contents* option allows you to recursively delete a selected folder and its contents.
- ♦ The *Rename Directory* option allows you modify the name of a selected directory.
- ♦ The *Create Subdirectory* option allows you to create subdirectories in the selected directory.
- ♦ The *Create Symbolic Link* option allows you to create a symbolic link in the selected directory.

For information, see “[Viewing Details about Directories and Performing Actions on Them](http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/butlqph.html#butlrr)” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/butlqph.html#butlrr) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

NSS Volume Share Information

On the Share Information page (*Manage NCP Services > Manage Shares*, then click the *Information* (i) icon to the left of the NSS volume name), the following capabilities were added:

- ♦ Additional details about the volume are displayed, such as the sector size and loaded name spaces.
- ♦ For NSS volumes, the *Compression* option shows whether the Compression attribute is enabled for the volume.

NSS Volume Directory and File Listing

On an NSS volume’s Directory and File Listing page (*Manage NCP Services > Manage Shares*, then click the NSS volume name link), the following capabilities were added:

- ♦ The *Text Search* option allows you to search the content of files for a specified text string.

- ♦ The *File Search* option allows you to search for a file on the selected volume.
- ♦ The *Inventory* option generates an *NCP Volume Inventory* report with statistics about the files stored on a selected volume.
- ♦ The *Upload* option allows you to upload a file to the selected volume.

For information, see “Browsing Files and Performing Actions on NSS Volumes” (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/nssactions.html) in the *OES 11: Novell Remote Manager Administration Guide* (http://www.novell.com/documentation/oes11/mgmt_remotemgr_lx/data/front.html).

3 Migrating Novell Remote Manager from NetWare to OES 11

Novell Remote Manager for Novell Open Enterprise Server (OES) 11 Service Pack 2 (SP2) runs on servers with OES 11 services installed. This section contains information about the following:

- ♦ [Section 3.1, “Coexistence,” on page 21](#)
- ♦ [Section 3.2, “Migration,” on page 21](#)

3.1 Coexistence

- ♦ [Section 3.1.1, “Compatibility,” on page 21](#)
- ♦ [Section 3.1.2, “Coexistence Issues,” on page 21](#)

This section provides information regarding the compatibility and coexistence of Novell Remote Manager for OES 11 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 108](#) and [“Accessing an Existing Group” on page 109](#).

Configuring Novell Remote Manager is somewhat different on an OES server than a NetWare server. See [“Changing the HTTPSTKD Configuration” on page 37](#).

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 11 SP2: Dynamic Storage Technology Administration Guide](#).
- ♦ NCP (NetWare Control Protocol) server and NCP volumes (shares) on Linux POSIX file systems. For information, see [OES 11 SP2: NCP Server for Linux Administration Guide](#).

4 Managing a Virtualized Linux Server with Novell Remote Manager

Using Novell Remote Manager for Linux to access and manage a virtualized Novell 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.

To get started with Xen virtualization, see the *Virtualization with Xen* (http://www.suse.com/documentation/sles11/book_xen/data/book_xen.html).

To get started with KVM virtualization, see the *Virtualization with KVM* (http://www.suse.com/documentation/sles11/book_kvm/data/book_kvm.html).

For information about setting up virtualized OES 11, see “Installing, Upgrading, or Updating OES on a VM” in the *OES 11 SP2: 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.

5 Installing Novell Remote Manager for Linux

Novell Remote Manager is installed as a Novell Open Enterprise Server (OES) 11 SP2 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 25](#)
- ♦ [Section 5.2, “Installing Novell Remote Manager After the Initial Server Installation,” on page 25](#)

5.1 Installing Novell Remote Manager During the Initial Server Installation

To install Novell Remote Manager during the installation of OES 11 SP2 or while adding OES 11 SP2 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 37](#).

For a list of RPMs that it installs, see [Appendix B, “Novell Remote Manager Packages,” on page 185](#).

5.2 Installing Novell Remote Manager After the Initial Server Installation

If you did not install Novell Remote Manager when you first installed OES 11 SP2, 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 Novell Open Enterprise Server Configuration summary page. When all the settings on the Novell 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 37.

For a list of RPMs that it installs, see [Appendix B, “Novell Remote Manager Packages,”](#) on page 185.

6 Accessing Novell Remote Manager for Linux

This section includes information about the following:

- ♦ [Section 6.1, “System Requirements,” on page 27](#)
- ♦ [Section 6.2, “Accessing Novell Remote Manager,” on page 28](#)
- ♦ [Section 6.3, “Starting or Stopping HTTPSTKD,” on page 30](#)
- ♦ [Section 6.4, “Understanding the Layout of Novell Remote Manager,” on page 30](#)
- ♦ [Section 6.5, “Accessing Configuration Options,” on page 36](#)
- ♦ [Section 6.6, “Accessing Online Help,” on page 36](#)
- ♦ [Section 6.7, “Accessing Novell Web Pages,” on page 36](#)

6.1 System Requirements

☐ Supported web browsers:

- ♦ Mozilla Firefox 12 or later
- ♦ Microsoft Internet Explorer (IE) 8 and 9. IE 10 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 `httpstk` daemon, see [Section 6.3, “Starting or Stopping HTTPSTKD,” on page 30](#).

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 25](#).

For package details, see [“Novell Remote Manager Packages” on page 185](#).

- ❑ In order to view the graphical displays in the file system inventory report, Java must be installed on the machine you use to access Novell Remote Manager, and the browser must have Java and Javascript enabled.

In Java 7 Update 51 (Java JRE 1.7.0_51) and later, applets with self-signed or unsigned certificates are blocked by the Java default *Security* setting of *High*, or a setting of *Very High*. You can set the Java *Security* setting to *Medium* in order to allow the graphical display applet to run after presenting a security prompt. Other security warnings about unsigned certificates or self-signed certificates must also be addressed. For more information, see [Section 19.4, “Inventory Graphics Are Not Displayed in the Web Browser,”](#) on page 161.

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 11 SP2: Novell 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 11 SP2: Novell 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 20.1, “Security Features,” on page 167](#). 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`

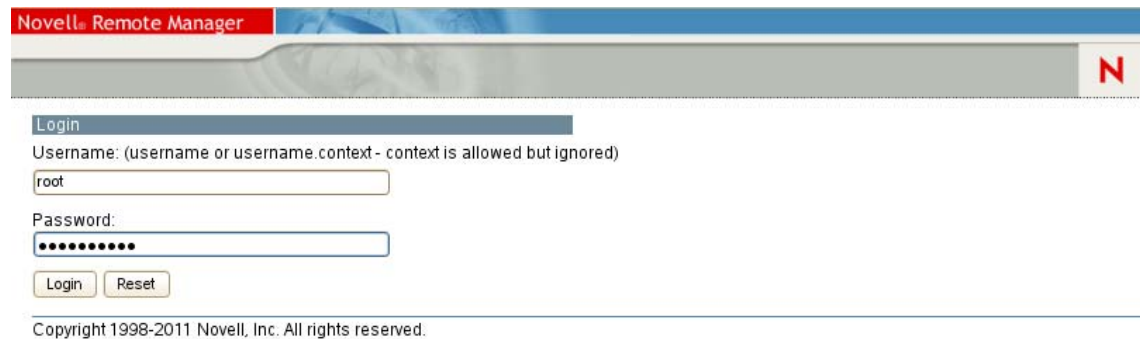
`https://172.16.123.11:8009`

- 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 30](#).

- 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) 11 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 6-1 *Commands for Starting, Stopping, or Checking the Status of Novell Remote Manager*

Task	Command
To see whether the module is running	<code>rcnovell-httpstkd status</code>
	or
	<code>/etc/init.d/novell-httpstkd status</code>
To restart HTTPSTKD	<code>rcnovell-httpstkd restart</code>
	or
	<code>/etc/init.d/novell-httpstkd restart</code>
To start HTTPSTKD	<code>rcnovell-httpstkd start</code>
	or
	<code>/etc/init.d/novell-httpstkd start</code>
To stop HTTPSTKD	<code>rcnovell-httpstkd stop</code>
	or
	<code>/etc/init.d/novell-httpstkd stop</code>

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 31](#) shows the overall layout of Novell Remote Manager for OES 11 SP2. [Figure 6-2 on page 32](#) shows the overall layout of Novell Remote Manager for OES 11 SP1 and earlier. For OES 11 SP2, 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

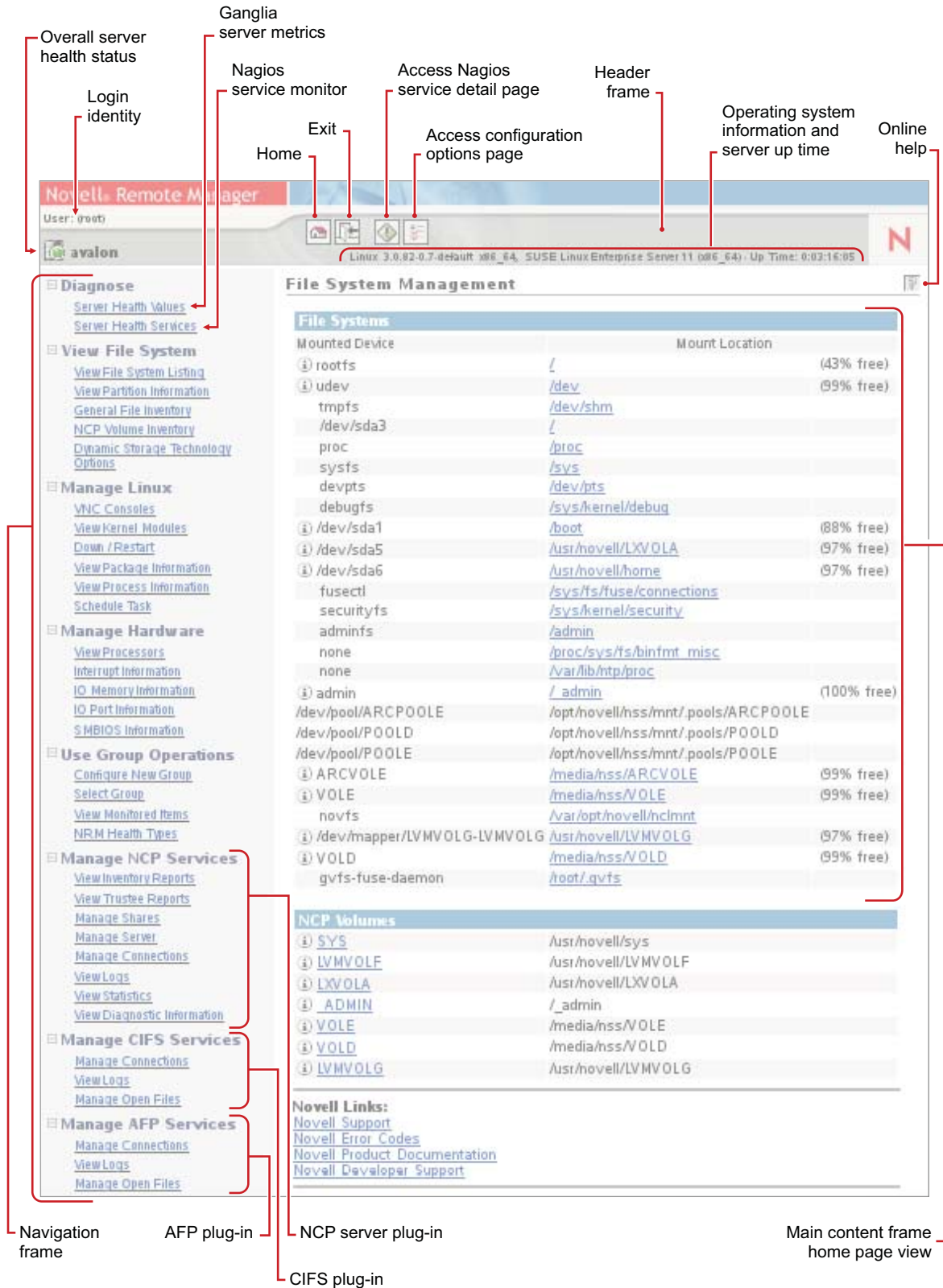
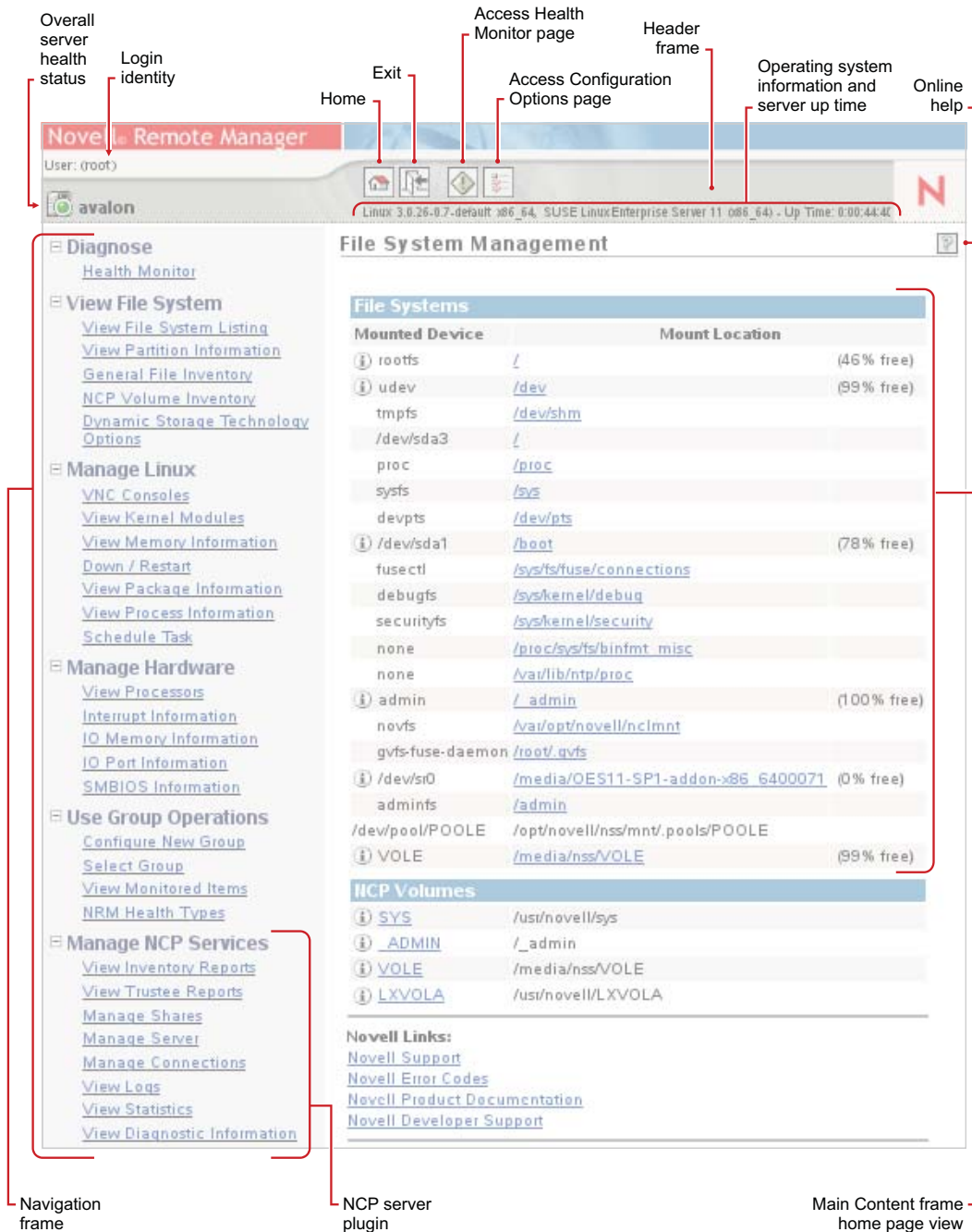


Figure 6-2 Layout of Novell Remote Manager for OES 11 SP1 and Earlier

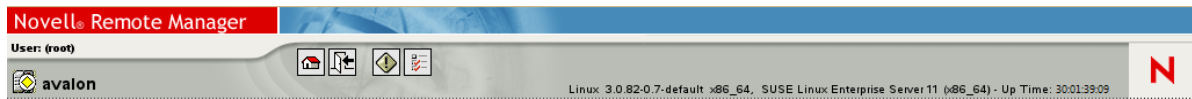


See the following sections for more information about the layout of the Novell Remote Manager Home page:

- Section 6.4.1, "Header Frame," on page 33
- Section 6.4.2, "Overall Health Indicator," on page 33
- Section 6.4.3, "Navigation Frame," on page 34
- Section 6.4.4, "Program Plug-Ins in the Navigation Frame," on page 35
- Section 6.4.5, "Main Content Frame," on page 35
- Section 6.4.6, "Online Help," on page 36

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.

- ◆  *Nagios Service Detail* (Health Monitor in OES 11 SP1 and earlier)


For information about configuring and using Nagios to monitor services, see [Section 8.5, “Configuring Nagios,”](#) on page 53.

- ◆  *Configuration*

For information about Novell Remote Manager configuration settings, see [Chapter 7, “Changing the HTTPSTKD Configuration,”](#) on page 37.

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 \(http://www.novell.com/support\)](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 11 SP2, 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 53](#).

For OES 11 SP1 and earlier, the status is determined by the state of selected services on the Health Monitoring page. The indicator changes if any selected 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 to go to the Health Monitor page and view the health statistics and alerts for services. For information about the using the Health Monitor, see [Chapter 9, “Diagnosing Problems Using Health Monitor \(OES 11 SP1\),” on page 69](#).

Table 6-2 Overall Server Health Status Conditions

Overall Health Status	Server Health Icon	Icon Description
Good		Green orb in a white circle
Suspect		Yellow diamond in a white circle
Bad		Red bar in a white circle
No connection to the server		Black X in a white circle

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

Roles	Description	For more information, see
Diagnose	Monitor the health of the server and services.	Chapter 8, “Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2),” on page 45 Chapter 9, “Diagnosing Problems Using Health Monitor (OES 11 SP1),” on page 69
View File System	Browse the file system, view information about files, folders, and partitions, and generate inventories.	Chapter 10, “Viewing File Systems,” on page 77

Roles	Description	For more information, see
Manage Linux	View information about kernel modules, packages, and processes. Schedule CRON jobs.	Chapter 11, “Managing Linux,” on page 85
Manage Hardware	View information about processors, interrupts, memory, ports, and SMBIOS.	Chapter 12, “Managing Hardware,” on page 97
Use Group Operations	Configure groups of servers to be monitored collectively.	Chapter 13, “Using Group Operations,” on page 103

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 6-4 Program Plug-In Roles in the Navigation Frame

OES Service	Roles in the Navigation Frame	For more information, see
NCP Server and Dynamic Storage Technology	<i>Manage NCP Services</i> allows you to manage NSS volumes, NCP volumes, DST volumes, NCP volume inventories, and NCP connections on the server.	Chapter 14, “Managing NCP Services,” on page 117 OES 11 SP2: NCP Server for Linux Administration Guide
	<i>Dynamic Storage Technology Options</i> allows you to configure and manage Dynamic Storage Technology volumes and policies. The DST functions are integrated with <i>Manage NCP Services</i> .	Chapter 15, “Managing Dynamic Storage Technology Options,” on page 143 OES 11 SP2: Dynamic Storage Technology Administration Guide
Novell CIFS	<i>Manage CIFS Services</i> allows you to manage Novell CIFS connections on the server.	Chapter 16, “Managing CIFS Services,” on page 147 OES 11 SP2: Novell CIFS for Linux Administration Guide.
Novell AFP	<i>Manage AFP Services</i> allows you to manage Novell AFP connections on the server.	Chapter 17, “Managing AFP Services,” on page 151 OES 11 SP2: Novell AFP for Linux Administration Guide


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 Configuration 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)
- ♦ Restart the Nagios daemon
- ♦ Restart the httpstkd daemon
- ♦ HTTP Logs
- ♦ Certificate Management
- ♦ Enable/disable the httpstkd daemon core file

For information about setting options, see [Chapter 7, “Changing the HTTPSTKD Configuration,” on page 37](#).

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 \(http://www.novell.com/support/\)](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 \(http://www.novell.com/documentation/nwec/index.html\)](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 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) links directly to the product documentation for all shipping Novell products.
- ♦ [Novell Developer Support \(http://www.novell.com/developer/\)](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.

7 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 11 SP2, 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 53](#).

Figure 7-1 The Novell Remote Manager Configuration Options Page

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 cgi config file](#)

[Edit Nagios command config 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 39
- ♦ Section 7.2, “Accessing and Editing the HTTPSTKD PAM Configuration File,” on page 40
- ♦ Section 7.3, “Restarting the HTTPSTKD Daemon,” on page 41
- ♦ Section 7.4, “Viewing the HTTP Logs,” on page 41
- ♦ Section 7.5, “Viewing and Creating Certificates for Novell Remote Manager,” on page 41
- ♦ Section 7.6, “Extending the eDirectory Schema for Novell Remote Manager Group Operations,” on page 42

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 41](#). You can also restart it manually as described in [Section 6.3, “Starting or Stopping HTTPSTKD,” on page 30](#).

[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

Functionality	Information about How to Change
Which network adapter Novell Remote Manager is bound to or add additional IP address that it is bound to	Section A.1, “Address and Port Commands,” on page 174
The certificates Novell Remote Manager is using for authentication	<ul style="list-style-type: none">♦ Section 7.5, “Viewing and Creating Certificates for Novell Remote Manager,” on page 41♦ Section A.1, “Address and Port Commands,” on page 174
The cipher strength of the SSL key that is used to access Novell Remote Manager	Section A.9, “SSL Key Cipher Strength Command,” on page 182
The <code>HttpOnly</code> attribute for cookies in a response header	Section A.5, “HttpOnly Command,” on page 178
The <code>InventoryResolveNonLumOwnerName</code> option for resolving names of NSS volume file owners if their eDirectory user names are not LUM enabled	Section A.6, “InventoryResolveNonLumOwnerName Command,” on page 179
Which plug-ins are loaded	Section A.8, “Load Command,” on page 181
Which workstations can access Novell Remote Manager	Section A.4, “Filtering Commands,” on page 177
For OES 11 SP1 and earlier, whether an email notification is sent for the Health Monitor tool or who receives it	Section A.3, “Email Notification Commands (OES 11 SP1 and Earlier),” on page 176

Functionality	Information about How to Change
Which users can log in to Novell Remote Manager	<ul style="list-style-type: none"> ♦ Section A.2, “Disable Auto LUM Command,” on page 175 ♦ Section A.10, “Supervisor Only Command,” on page 182
The language the browser supports	Section A.7, “Language Commands,” on page 179

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 41](#).

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 41](#).

For more information about the PAM configuration file and the options available, see [“Authentication with PAM”](#) (http://www.suse.com/documentation/sles11/book_security/data/cha_pam.html) in the *SUSE Linux Enterprise Server 11 Security Guide* (http://www.suse.com/documentation/sles11/book_security/data/book_security.html).

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 30](#).


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 the NDS Schema for NRM* 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.

8 Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2)

Novell Remote Manager includes several tools to assist you in monitoring the health and status of your server and services. Beginning in Novell Open Enterprise Server (OES) 11 SP2, 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 11 SP2. It is replaced by the Ganglia and Nagios open source monitoring tools, which do not use the Small Footprint CIM Broker (SFCB) for communications.

For information about using the Health Monitor function in OES 11 SP1 and earlier, see [Chapter 9, “Diagnosing Problems Using Health Monitor \(OES 11 SP1\),”](#) on page 69.

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 46
- ♦ [Section 8.2, “Configuring Ganglia,”](#) on page 47
- ♦ [Section 8.3, “Stopping and Starting Ganglia gmond and gmetad,”](#) on page 50
- ♦ [Section 8.4, “Monitoring Server Health with Ganglia,”](#) on page 50
- ♦ [Section 8.5, “Configuring Nagios,”](#) on page 53
- ♦ [Section 8.6, “Monitoring Service Health with Nagios,”](#) on page 60
- ♦ [Section 8.7, “Restarting Nagios,”](#) on page 61
- ♦ [Section 8.8, “Managing Nagios Users,”](#) on page 61
- ♦ [Section 8.9, “Modifying the Nagios Notification Methods for Contacts,”](#) on page 64
- ♦ [Section 8.10, “Configuring Nagios Logging,”](#) on page 64
- ♦ [Section 8.11, “Viewing the PIDs or Monitoring the Health of Processes,”](#) on page 66
- ♦ [Section 8.12, “Monitoring or Killing an Individual Process,”](#) on page 67
- ♦ [Section 8.13, “Troubleshooting a Suspect or Bad Health Status,”](#) on page 68

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 46](#)
- [Section 8.1.2, “Setting the Health Status Refresh Rate,” on page 46](#)

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 8-1 *Server Health Status*

Icon	Server Health Status	Explanation
	Good	All parameters included in the server's health configuration list are good.
	Suspect	The status of one or more of the parameters included in the server's health configuration list is suspect or has a minor problem.
	Bad	The status of one or more of the parameters included in the server's health configuration list is bad or has a critical problem.
	Lost connection	The connection to the server from Novell Remote Manager has been lost.

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 47](#)
- ♦ [Section 8.2.2, “Configuring Ganglia gmond in Multicast Mode or Unicast Mode,” on page 48](#)

8.2.1 Ganglia Requirements

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

- ♦ [“Port 8649” on page 47](#)
- ♦ [“Time Synchronization” on page 47](#)

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

```
SuSEfirewall12 open EXT UDP 8649
SuSEfirewall12 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-robin 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

```
SuSEfirewall12 open EXT UDP 123
```

- 3 Configure NTP on the server.

For information about configuring NTP, see “Time Services” in the *OES 11 SP2: 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* (<http://sourceforge.net/apps/trac/ganglia/>) website.

- “Using Ganglia in Multicast Mode” on page 48
- “Using Ganglia in Unicast Mode” on page 49
- “Configuring gmond for Server-Centric Monitoring” on page 49

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 49](#).

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.

For more information about configuring Ganglia in unicast mode, see the [Ganglia Quick Start Guide](http://sourceforge.net/apps/trac/ganglia/wiki/ganglia_quick_start) (http://sourceforge.net/apps/trac/ganglia/wiki/ganglia_quick_start) on the [Ganglia Project](http://sourceforge.net/apps/trac/ganglia/) (<http://sourceforge.net/apps/trac/ganglia/>) website.

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
    host = <server_hostname>
    port = 8649
    #ttl = 1
}
```

You comment out the `mcast_join` parameter and the `ttl` parameter.

You add the `host` parameter and set it to the hostname for the server, such as `avalon`. You can get the server's host name from the command line with the following command:

```
hostname --fqdn
```

- 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`:

```
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

```
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 Frontend 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:

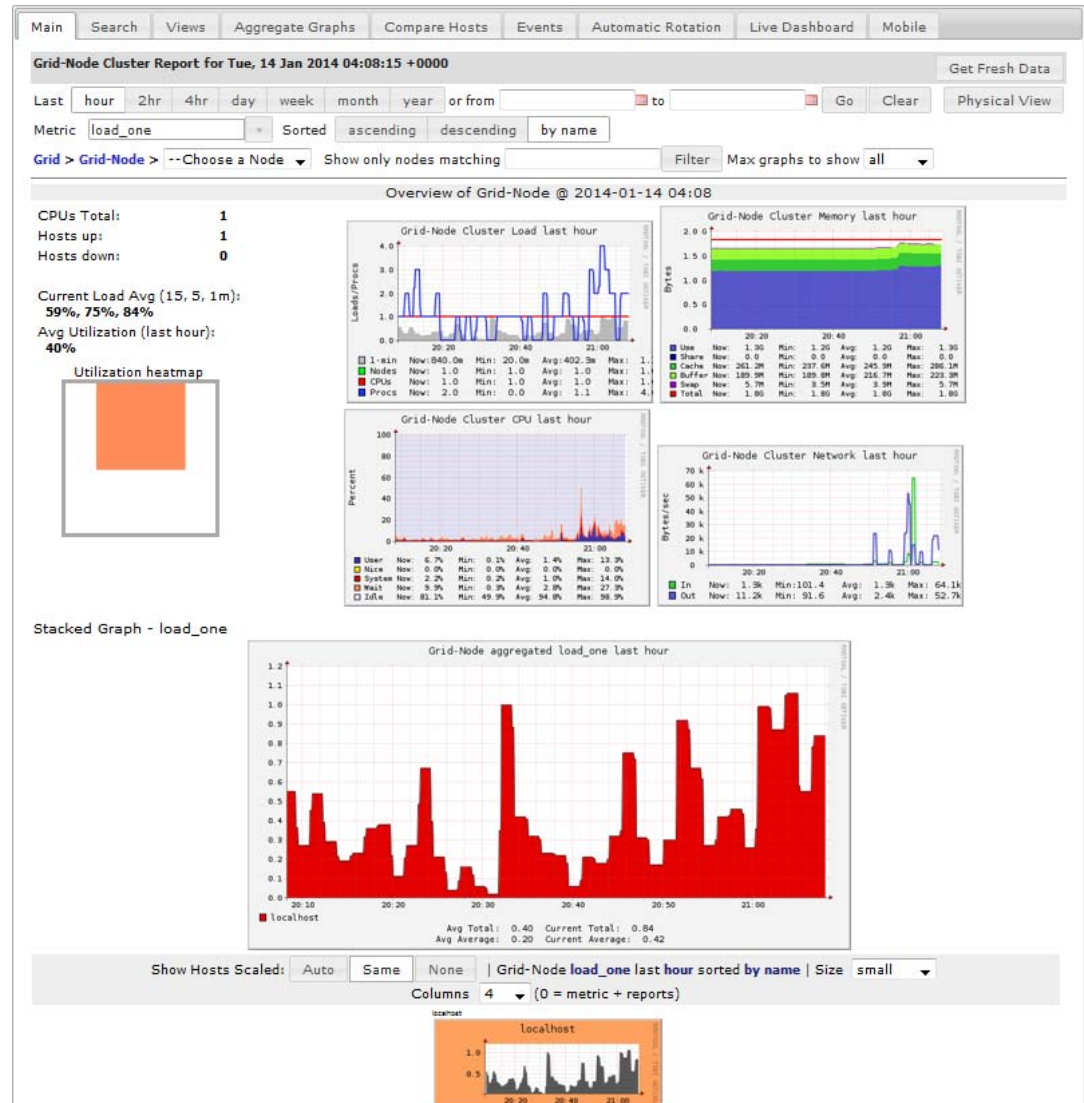
- ♦ Log in to Novell Remote Manager as the Linux `root` user or as a LUM-enabled administrator user.
- ♦ Select *Diagnose > Server Health Values* to go to the Ganglia main dashboard. Continue to [Step 2 on page 51](#).

or

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



```
http://<server_ip_address>/gweb
```

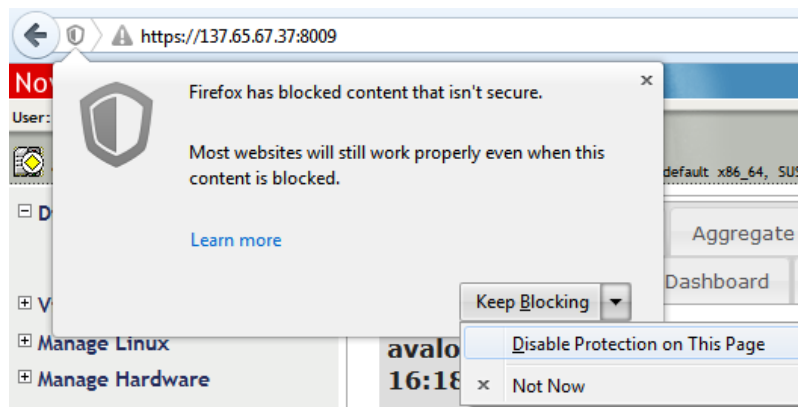
Continue to [Step 3 on page 53](#).



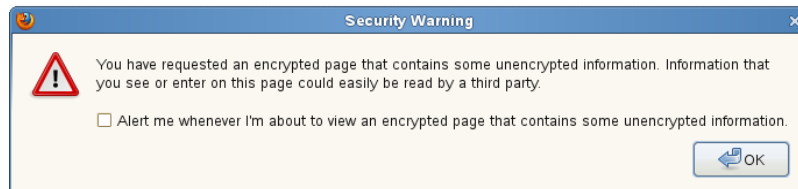
- 2 If you are prompted with a security warning that the page contains mixed content (both secure and non-secure elements), select the option to show all content.

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.

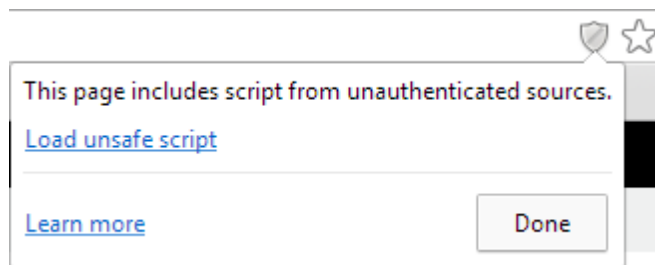




A round shield icon replaces the lock to the left of the `https://` in the address bar. Right-click the icon to view the message that advises: Your connection to this site is only partially encrypted, and does not prevent eavesdropping.

- ♦ **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 .

3 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 53](#)
- ♦ [Section 8.5.2, “Configuring Nagios Monitoring,” on page 57](#)
- ♦ [Section 8.5.3, “Accessing the Nagios Website,” on page 59](#)
- ♦ [Section 8.5.4, “Using Nagios Plug-Ins,” on page 59](#)
- ♦ [Section 8.5.5, “Using Object Configuration Files,” on page 60](#)
- ♦ [Section 8.5.6, “Additional Information,” on page 60](#)

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 54](#)
- ♦ [“Setting or Modifying an Email Address for the nagiosadmin Contact” on page 55](#)
- ♦ [“Using the Nagios admins Contact Group” on page 57](#)

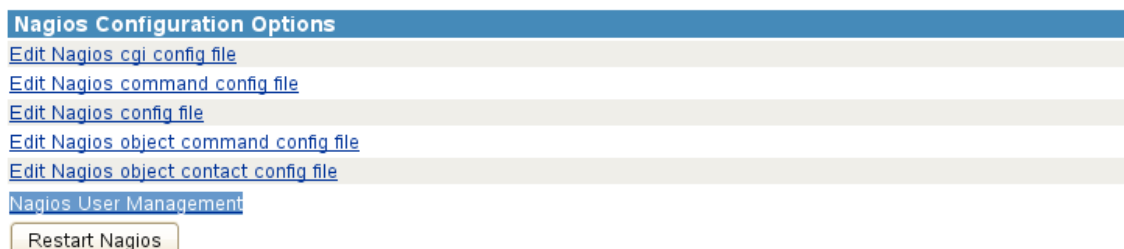
Setting or Modifying the Password for the nagiosadmin User

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.
- 3 Under *Nagios Configuration Options*, click *Nagios User Management*.



- 4 On the Nagios User Management page, specify nagiosadmin as the Nagios user name.

A screenshot of the 'Nagios User Management' page. It has a blue header with the title and a help icon. Below the header is a section titled 'Nagios User Information'. This section contains three input fields: 'Nagios Username' with the value 'nagiosadmin', 'Nagios Password' with masked characters, and 'Confirm Nagios Password' with masked characters. Below these fields are two buttons: 'Create User' and 'Delete User'.

- 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

Nagios User Information

The username **nagiosadmin** was created with the entered password for use in Nagios.

OK

For information about configuring additional Nagios users and the tasks they can perform, see [Section 8.8, “Managing Nagios Users,”](#) on page 61.

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 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.

Nagios Configuration Options

[Edit Nagios cgi config file](#)

[Edit Nagios command config file](#)

[Edit Nagios config file](#)

[Edit Nagios object command config file](#)

[Edit Nagios object contact config file](#)

[Nagios User Management](#)

Restart Nagios

- 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`.

```

/etc/nagios/objects/contacts.cfg
#####
#
# CONTACTS
#
#####
# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the 'generic-
# contact'
# template which is defined elsewhere.

define contact{
    contact_name      nagiosadmin      ; Short name of user
    use               generic-contact   ; Inherit default
    values from generic-contact template (defined above)
    alias             Nagios Admin     ; Full name of user
    email             bob@example.com ; <<***** CHANGE THIS TO
    YOUR EMAIL ADDRESS *****
}

#####
Save Changes File Encoding: ☒ ANSI ☐ UTF-8

```

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.

/etc/nagios/objects

Upload Text Search Inventory

Directory Listing				
Info	Name	Size	Date and time	Attributes
	.	N/A	Thu 09 Jan 2014 09:37:55 PM MST	d_rwx_rwx_r_x
	.	N/A	Mon 13 Jan 2014 12:26:32 PM MST	d_rwx_rwx_r_x
	commands.cfg	7,710	Mon 11 Feb 2013 01:46:01 PM MST	_rw_rw_r_
	contacts.cfg	2,167	Mon 13 Jan 2014 12:26:32 PM MST	_rw_rw_r_

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.

Are you sure you want to restart Nagios? (Services provided by Nagios will temporarily be disabled.)

Cancel
OK

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*

Nagios Configuration Option	Related File or Command	Description
Edit Nagios cgi config file	<code>/etc/nagios/cgi.cfg</code>	Defines the CGI parameters and which contacts or contact groups are allowed to access them.
Edit Nagios command config file	<code>/etc/nagios/command.cfg</code>	Defines commands, including service check, service notification, host check, host notification, service event handler, and host even handler.
Edit Nagios config file	<code>/etc/nagios/nagios.cfg</code>	<p>Specifies the main log file where service and host events are logged. For more information, see Section 8.10, “Configuring Nagios Logging,” on page 64.</p> <p>You can configure other Nagios parameters as defined in the configuration file.</p>
Edit Nagios object command config file	<code>/etc/nagios/objects/commands.cfg</code>	Provides you with some sample command definitions that you can reference in host, service, and contact definitions.

Nagios Configuration Option	Related File or Command	Description
Edit Nagios object contact config file	<code>/etc/nagios/objects/contacts.cfg</code>	<p>By default, defines the nagiosadmin user as a contact and adds the contact to the contact group admins. You must specify an email address to use for alert notifications sent to the nagiosadmin contact.</p> <p>You can configure Nagios users as contacts and set up contact methods for each one, such as email, pager, cell phone, instant message, audio alert, and so on.</p> <p>You can also add a contact as a member of the default contact group admins, or create other contact groups and add contacts as members.</p>
Nagios User Management	<code>/etc/nagios/htpasswd.users</code>	<p>Create a Nagios user name and password, or delete a Nagios user. You can also use this option to create the user name with a different password.</p> <p>For more information, see Section 8.8, "Managing Nagios Users," on page 61.</p>
Restart Nagios	<code>rcnagios restart</code>	Restart the Nagios daemon after you make changes to the configuration files.

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.

You might see an Apache 403 Forbidden Warning error reported in Nagios after a new installation or upgrade to OES 11 SP2. For resolving this issue, see [Section 19.3, “Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 11 SP2,”](#) on page 160.

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>/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 \(http://exchange.nagios.org/\)](http://exchange.nagios.org/) website. Currently, OES 11 SP2 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 \(http://www.nagios-plugins.org/doc/index.html\)](http://www.nagios-plugins.org/doc/index.html) on the [Nagios Plug-Ins Project \(http://www.nagios-plugins.org/\)](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](http://www.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.

For information on troubleshooting Nagios, see [Chapter 19, “Troubleshooting Novell Remote Manager,”](#) on page 159.



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 53.

You can also configure other Nagios users. For more information, see [Section 8.8, “Managing Nagios Users,”](#) on page 61.

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.

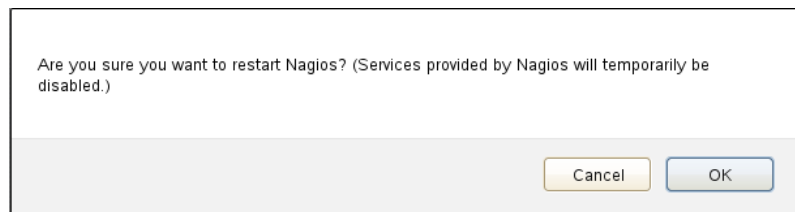
For information about setting up Nagios users, see [Section 8.8, “Managing Nagios Users,”](#) on [page 61](#).

- 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.
- 3 Under *Nagios Configuration Options*, click *Restart Nagios*.
- 4 When you are prompted to confirm the restart, click *OK* to proceed.



- 5 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.

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 62](#)
- ♦ [Section 8.8.2, “Setting Passwords for Nagios Users,”](#) on [page 62](#)
- ♦ [Section 8.8.3, “Deleting a Nagios User,”](#) on [page 62](#)
- ♦ [Section 8.8.4, “Configuring Nagios Contacts and Notification Methods for Them,”](#) on [page 63](#)
- ♦ [Section 8.8.5, “Configuring Nagios CGI Authorization for Contacts,”](#) on [page 63](#)

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.
- 3 Under *Nagios Configuration Options*, click *Nagios User Management*.
- 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 63](#)
 - ♦ [Section 8.8.5, “Configuring Nagios CGI Authorization for Contacts,” on page 63](#)

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 61](#).
- 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 63](#).
- 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 55](#).

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 8-3 *Nagios Logging Options*

Logging Parameter	Description and Logging Options	Default Setting
<code>log_file</code>	Specifies the path of the log file, including the file name.	<code>/var/log/nagios/nagios.log</code>

Logging Parameter	Description and Logging Options	Default Setting
log_rotation_method	<p>Specifies the rotation method that Nagios should use to rotate its main log file, or disables rotation of the log.</p> <ul style="list-style-type: none"> ♦ 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 <code>nagios.log</code> 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.	<code>/var/log/nagios/archives</code>
use_syslog	<p>Specifies whether to log Nagios messages to the syslog facility as well as to the Nagios main log file.</p> <ul style="list-style-type: none"> ♦ 1: Enable messages to syslog. ♦ 0: Disable messages to syslog. 	Messages are sent to syslog as well as to <code>nagios.log</code> .
log_notifications	<p>Specifies whether to log notifications.</p> <ul style="list-style-type: none"> ♦ 1: Log notifications. ♦ 0: Do not log notifications. 	Log notifications.
log_service_retries	<p>Specifies whether to log service check retries.</p> <ul style="list-style-type: none"> ♦ 1: Log service check retries. ♦ 0: Do not log service check retries. 	Log service retries.
log_host_retries	<p>Specifies whether to log host check retries.</p> <ul style="list-style-type: none"> ♦ 1: Log host check retries. ♦ 0: Do not log host check retries. 	Log host check retries.
log_event_handlers	<p>Specifies whether to log host and service event handlers.</p> <ul style="list-style-type: none"> ♦ 1: Log host and service event handlers. ♦ 0: Do not log host and service event handlers. 	Log host and service event handlers.

Logging Parameter	Description and Logging Options	Default Setting
log_initial_states	<p>Specifies whether to log the initial state for every host and service the first time its status is checked. Enable this option only if you are using an external application that reports its long-term state statistics.</p> <ul style="list-style-type: none"> ♦ 1: Log the initial state for every host and service. ♦ 0: Do not log the initial state for every host and service. 	Do not log the initial state for every host and service.
log_external_commands	<p>Specifies whether to log external commands.</p> <ul style="list-style-type: none"> ♦ 1: Log external commands. ♦ 0: Do not log external commands. <p>NOTE: The <code>check_external_commands</code> option is enabled by default for Novell Remote Manager. This enables you to use the CGI command interface.</p> <p>The <code>command_check_interval</code> is set to -1 by default for Novell Remote Manager. This causes Nagios to check the external command file as often as possible.</p>	Log external commands.
log_passive_checks	<p>Specifies whether to log passive host and service checks.</p> <ul style="list-style-type: none"> ♦ 1: Log passive checks. ♦ 0: Do not log passive checks. 	Log passive checks.

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 8-4 Process Health Information

Parameter	Description
Process Information	Shows an <i>Information</i> icon. Click the <i>Information</i> icon next to the process name to monitor or kill an individual process. For information, see Section 9.3, "Monitoring or Killing an Individual Process," on page 75.
Name	Shows the process or executable program name.
Owner	Shows the process owner (the user who started the process).

Parameter	Description
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: <ul style="list-style-type: none"> ♦ < 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 <code>top</code> 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 <code>top</code> command's RSS switch. The Linux <code>top</code> 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

Parameter	Description
Process Name	Shows the process or executable program name.
Process ID	Shows the process identifier.
Status	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.
Command Line	Shows the actual command line of the executed command to start this process.
Working Directory	Shows the current working directory of the process.
Executable Path	Shows the actual path name of the executed command to start this process.
Total Memory	Shows the total memory allocated to this process.
Code Size	Shows the total memory allocated for code to this process.

Parameter	Description
Data Size	Shows the total memory allocated for data to this process.
Library Memory	Shows the total memory allocated for libraries to this process.
Dirty Pages	Shows the total memory that is dirty that belongs to this process.
Resident Pages	Shows the amount of memory that this process is using that has not been swapped out.
Tasks	Shows a list of tasks or threads belonging to this process.
File Descriptors	Shows a list of file descriptors that the process has open.

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.

9 Diagnosing Problems Using Health Monitor (OES 11 SP1)

Novell Remote Manager for Novell Open Enterprise Server 11 SP1 and earlier includes several tools to assist you in monitoring the health and status of your server. When you are familiar with the normal health and status of your server, diagnosing problems with your server becomes easier.

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

- ♦ [Section 9.1, “Monitoring Server Health,” on page 69](#)
- ♦ [Section 9.2, “Viewing the PIDs or Monitoring the Health of Processes,” on page 74](#)
- ♦ [Section 9.3, “Monitoring or Killing an Individual Process,” on page 75](#)
- ♦ [Section 9.4, “Troubleshooting a Suspect or Bad Health Status,” on page 75](#)

9.1 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. Monitoring your server’s health involves the following tasks:

- ♦ [Section 9.1.1, “Accessing the Health Monitor,” on page 69](#)
- ♦ [Section 9.1.2, “Viewing the Health Monitor,” on page 70](#)
- ♦ [Section 9.1.3, “Monitoring Overall Server Health or the Health of a Specific Item,” on page 70](#)
- ♦ [Section 9.1.4, “Configuring the Items to Monitor,” on page 73](#)
- ♦ [Section 9.1.5, “Configuring Email Notification for Server Health Status,” on page 74](#)

9.1.1 Accessing the Health Monitor

The Health Monitor page allows you to monitor your server's overall health, configure which items determine the server's overall health status, and configure which items you want to be notified about.

To access the Health Monitor page, click one of the following links in Novell Remote Manager:

- ♦  *Overall server health status indicator icon*
- ♦  *Health Monitor icon in the header frame*
- ♦ *Diagnose > Health Monitor link in the navigation frame*

9.1.2 Viewing the Health Monitor

The Health Monitor page reports information about the operating system and the services that are running on the operating system as shown in [Figure 9-1](#). You can use this page to monitor your server's overall health, configure which items determine the server's overall health status, and configure which items you want to be notified about.

Figure 9-1 Novell Remote Manager Health Monitor

Novell Remote Manager

User: (root)

longbourn Linux 3.0.38-0.5-default x86_64, SUSE Linux Enterprise Server 11 (x86_64) - Up Time: 0:00:21:33

Diagnose

- Health Monitor
- View File System
- Manage Linux
- Manage Hardware
- Use Group Operations
- Manage NCP Services

Health Monitor

Begin Refresh Page Refresh Rate 10 seconds

Operating System							
Status	Description	Current	Peak	Max	Info	Include	Notify
●	CPU Utilization	4294960996	4294967196	100	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	Process Count	292	294	N/A	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	Physical Memory	70 MB	*53 MB	930 MB	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	Swap Memory	992 MB	*992 MB	1,027 MB	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	Virtual Memory	1,255 MB	*1,247 MB	1,958 MB	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	LAN Collisions	0	0	N/A	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>

*Low Value

Apply Settings

Services					
Status	Description	Mode	Info	Include	Notify
●	novell-tomcat6	Running	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	ntp	Running	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	adminfs	Running	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
○	ipmi	Stopped	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	cron	Running	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
○	splash	Stopped	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	avahi-daemon	Running	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
○	atd	Stopped	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	ndsd	Running	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>
●	autoyast	Running	i	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Apply Settings

9.1.3 Monitoring Overall Server Health or the Health of a Specific Item

Using Novell Remote Manager, you can monitor the server's overall health and the health of a specific item.

- ◆ [“Overall Server Health Status” on page 71](#)
- ◆ [“Health Status Refresh Rate” on page 71](#)

- ♦ “Operating System Health” on page 72
- ♦ “Services Health” on page 73

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 9-1 *Server Health Status*

Icon	Server Health Status	Explanation
	Good	All parameters included in the server's health configuration list are good.
	Suspect	The status of one or more of the parameters included in the server's health configuration list is suspect or has a minor problem.
	Bad	The status of one or more of the parameters included in the server's health configuration list is bad or has a critical problem.
	Lost connection	The connection to the server from Novell Remote Manager has been lost.

The server’s overall health is determined by items that are selected in the *Include* list on the detailed Health Monitor page as shown in [Figure 9-1, “Novell Remote Manager Health Monitor,” on page 70](#). By default, all items are selected. The items represent the processes that are loaded on the server.

If the status of any item that is selected in the *Include* list 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).

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.

Operating System Health

The *Operating System* table on the Health Monitor page shows the health status (green/good, yellow/suspect, or red/bad) for all known components of the operating system, as well as current, peak, and maximum values. When an item is not selected in the *Include* list, it is not included when determining the overall server health and the values for *Status*, *Current*, *Peak*, and *Max* are not displayed.

The following items in the *Operating System* table are key indicators of your server's health:

- ♦ CPU Utilization (for each processor, if there is more than one)
- ♦ Process Count

For information about monitoring processes, see [Section 9.2, "Viewing the PIDs or Monitoring the Health of Processes," on page 74](#) and [Section 9.3, "Monitoring or Killing an Individual Process," on page 75](#).

- ♦ Physical Memory
- ♦ Swap Memory
- ♦ Virtual Memory
- ♦ LAN Collisions

IMPORTANT: You must click the *Apply Settings* button below the *Operating System* table to apply your changes to values in that table. If you leave the page without applying the changes, the settings return to their saved values.

You cannot change the thresholds for the *Suspect* and *Critical* values of these indicators. See the online help for each parameter to see the set thresholds.

[Table 9-2](#) describes the information that is provided for each of the operating system components:



Table 9-2 *Operating System Health Information*

Parameter	Description
Status	For specific details regarding the status indicator of an item, click the Information icon for that item.
Description	A list of resources, processes, or items that can affect the health of your server. When you want to see the specific details or status for an item, click the description name for that item.
Current	Represents the current value being reported for the item's specific health status. For current memory, the value is the total amount of free memory that was available when the server was recently polled.
Peak	Represents the highest value reported for the item's specific health status since the server was started. For peak memory, the peak value is the least amount of memory that has been available while Novell Remote Manager has been running. It reports the amount of free memory available when the server's memory usage peaked during the observed interval.
Max	Represents the highest value possible for the item's specific health status. For maximum memory, the value is the total amount of memory in the system.

Parameter	Description
Info	For specific details regarding the status indicator, settings, or meaning of an item, click the Information icon for that item.
Include	When you want to include an item in determining the overall health status of your server, check the check box for that item. By default, all items are checked. When an item is not checked, it is not included when determining the overall server health; nor are its values for Status, Current, Peak, and Max displayed.
Notify	<p>When you want to be notified about a status of an item, check the check box for that item. You will be notified when the status changes.</p> <p>Before you can receive notifications, you must also configure email addresses in the <code>/etc/opt/novell/httpstkd.conf</code> file. You can edit this file via the link provided on the Configuration page. Restart <code>httpstkd</code> after making these changes by executing the following command on the Linux server as the <code>root</code> user:</p> <pre>/etc/init.d/novell-httpstkd restart</pre>

Services Health

The *Services* table on the Health Monitor page also shows the health status of the services installed on the server as well as their online or offline status. When a service is offline, the health status of the service is not included in the server's overall health whether or not it is selected in the *Include* list.

The mode indicates that the server is running  or stopped . To change the mode of the service, click the mode link for that service. The mode page opens for the service where you can start, stop, or restart the service by clicking the applicable button.

You can modify the *Include* and *Notify* settings in the *Services* table by selecting and deselecting the check boxes in those columns, then clicking *Apply Settings* below the table.

IMPORTANT: You must click the *Apply Settings* button below the *Services* table to apply your changes to values in that table. If you leave the page without applying the changes, the settings return to their saved values.

9.1.4 Configuring the Items to Monitor

As stated in the previous section, the server's overall health is determined by items that are selected in the *Include* list on the detailed Health Monitor page. By default, all of the items are selected.

Therefore, if you have a server that has specific parameters that you know will cause a suspect or bad status and you want to be notified only when other parameters have changed, you can remove the items with the suspect or bad parameters from the *Include* and *Notify* lists by deselecting them and clicking *Apply Settings*. You need to apply the settings for the Services items separately from the Operating System items.

9.1.5 Configuring Email Notification for Server Health Status

Rather than manually checking the status, you can configure Novell Remote Manager to send an email to notify you when the server's health status changes to any value other than green (good).

- 1 Select the *Notify* check box for the item on the Health Monitor page.
- 2 Specify the required information for email notification in the `/etc/opt/novell/httpstkd.conf` file.

You can edit this file via the link provided on the Configuration Options page.

- 3 After changing the `/etc/opt/novell/httpstkd.conf` file, restart HTTPSTKD.

Click the *Restart HTTPSTKD* button on the Configuration Options page or execute the following command in a console shell on the Linux server:

```
rcnovell-httpstkd restart
```

9.2 Viewing the PIDs or Monitoring the Health of Processes

On the Health Monitor , under *Operating System*, you can click the *Process Count* link to view a list of active processes. [Table 9-3](#) describes the health information that is reported for each process:

Table 9-3 *Process Health Information*

Parameter	Description
Process Information	Shows an <i>Information</i> icon. Click the <i>Information</i> icon next to the process name to monitor or kill an individual process. For information, see Section 9.3, "Monitoring or Killing an Individual Process," on page 75.
Name	Shows the process or executable program name.
Owner	Shows the process owner (the user who started the process).
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: <ul style="list-style-type: none">♦ < 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 <code>top</code> 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 <code>top</code> command's RSS switch. The Linux <code>top</code> command reports this information in kilobytes.

9.3 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 access the Process Information page in Novell Remote Manager:


- 1 Select *Diagnose > Health Monitor*.
- 2 Under Operating System, click *Process Count*.
- 3 Click the process Name link to view the Process Information page for the selected process.

Table 9-4 Process Information

Parameter	Description
Process Name	Shows the process or executable program name.
Process ID	Shows the process identifier.
Status	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.
Command Line	Shows the actual command line of the executed command to start this process.
Working Directory	Shows the current working directory of the process.
Executable Path	Shows the actual path name of the executed command to start this process.
Total Memory	Shows the total memory allocated to this process.
Code Size	Shows the total memory allocated for code to this process.
Data Size	Shows the total memory allocated for data to this process.
Library Memory	Shows the total memory allocated for libraries to this process.
Dirty Pages	Shows the total memory that is dirty that belongs to this process.
Resident Pages	Shows the amount of memory that this process is using that has not been swapped out.
Tasks	Shows a list of tasks or threads belonging to this process.
File Descriptors	Shows a list of file descriptors that the process has open.

9.4 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 the Health Monitor page.
- 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.

10 Viewing File Systems

The *Home* icon  and *View File Systems* section in Novell Remote Manager for Linux include the following links to these pages:

Table 10-1 *Links for Viewing File System Information*

Link	Page Displayed
<i>Home icon</i>	File System Management
<i>View File System Listing</i>	Directory Listing of / (root) directory
<i>View Partition Information</i>	Partition Information

From these pages you can perform the following tasks:

- ♦ [Section 10.1, “Viewing Mounted Devices and Performing Actions on Them,” on page 78](#)
- ♦ [Section 10.2, “Browsing File Systems and Performing Actions on Them,” on page 79](#)
- ♦ [Section 10.3, “Viewing Partition Information,” on page 83](#)

10.1 Viewing Mounted Devices and Performing Actions on Them

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

Figure 10-1 File System Management Page with Information Pages

File System Information


File System: /dev/hda2

Mount Point /

Type ext3

Size 31GB

In Use 3.3GB

Free Space  (88%, 26G Free)

File System Information


File System: AP/.CORE_OS.DEV.NOVELL

Mount Point /mnt/users

Type ncifs

Size 228GB

In Use 71GB

Free Space  (69%, 157G Free)

[Unmount](#)

File System Management

File Systems


Mounted Device	Mount Location	
rootfs	/	(88% free)
/dev/root	/	
proc	/proc	
sysfs	/sys	
devpts	/dev/pts	
tmpfs	/dev/shm	
/dev/dvd	/media/dvd	
/dev/fd0	/media/floppy	
usbfs	/proc/bus/usb	
AP/.CORE_OS.DEV.NOVELL	/mnt/code	(18% free)
AP/.CORE_OS.DEV.NOVELL	/mnt/users	(69% free)
DR/.CORE_OS.DEV.NOVELL	/mnt/data	(63% free)

NCP Volumes

SYS	/usr/novell/sys
-----	-----------------

SYS Share Information

Information															
Description	Value														
File system path	/usr/novell/sys														
File system type	EXT3														
NCP volume ID	0														
Status	mounted online														
Local cache	<table><thead><tr><th>Parameter</th><th>Value</th></tr></thead><tbody><tr><td>trustee count</td><td>2</td></tr><tr><td>cached files</td><td>2</td></tr><tr><td>evicted files</td><td>0</td></tr><tr><td>cached folders</td><td>35</td></tr><tr><td>cache retrieved</td><td>122</td></tr><tr><td>cache retrieved locked</td><td>2</td></tr></tbody></table>	Parameter	Value	trustee count	2	cached files	2	evicted files	0	cached folders	35	cache retrieved	122	cache retrieved locked	2
Parameter	Value														
trustee count	2														
cached files	2														
evicted files	0														
cached folders	35														
cache retrieved	122														
cache retrieved locked	2														

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 11 SP2: 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.

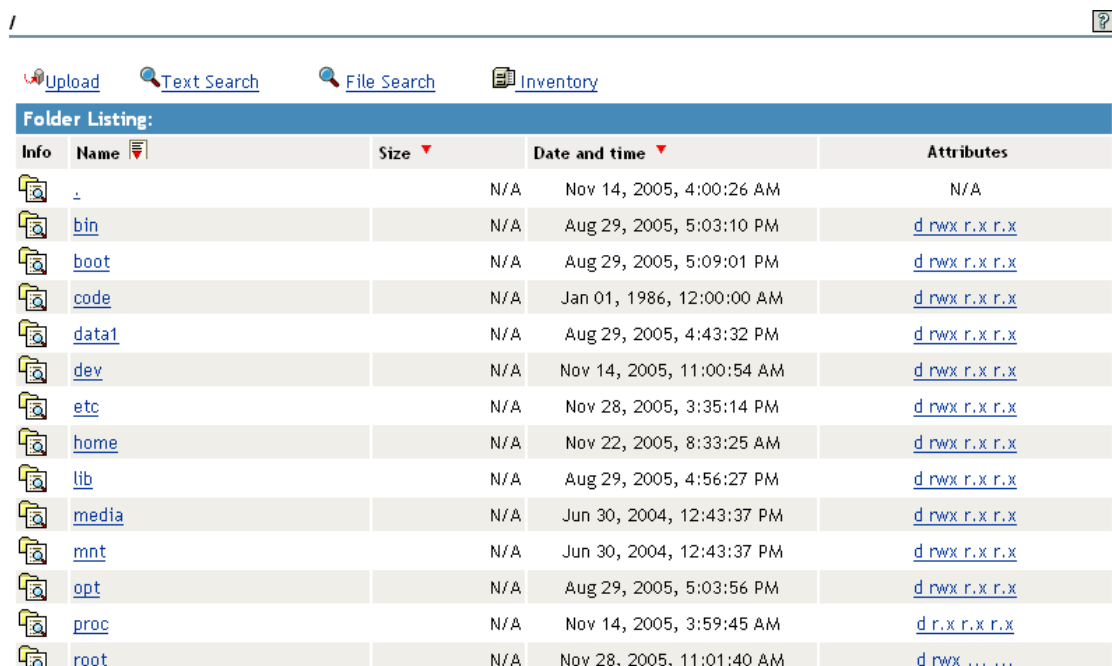
You can browse any of these file systems by clicking the link in the *Mount Location* column. At this point, you can perform any of the tasks listed for browsing the servers file system. See “[Browsing File Systems and Performing Actions on Them](#)” on page 79.

10.2 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.

Figure 10-2 Directory List Page



Folder Listing:				
Info	Name	Size	Date and time	Attributes
	.	N/A	Nov 14, 2005, 4:00:26 AM	N/A
	bin	N/A	Aug 29, 2005, 5:03:10 PM	d rwx r.x r.x
	boot	N/A	Aug 29, 2005, 5:09:01 PM	d rwx r.x r.x
	code	N/A	Jan 01, 1986, 12:00:00 AM	d rwx r.x r.x
	data1	N/A	Aug 29, 2005, 4:43:32 PM	d rwx r.x r.x
	dev	N/A	Nov 14, 2005, 11:00:54 AM	d rwx r.x r.x
	etc	N/A	Nov 28, 2005, 3:35:14 PM	d rwx r.x r.x
	home	N/A	Nov 22, 2005, 8:33:25 AM	d rwx r.x r.x
	lib	N/A	Aug 29, 2005, 4:56:27 PM	d rwx r.x r.x
	media	N/A	Jun 30, 2004, 12:43:37 PM	d rwx r.x r.x
	mnt	N/A	Jun 30, 2004, 12:43:37 PM	d rwx r.x r.x
	opt	N/A	Aug 29, 2005, 5:03:56 PM	d rwx r.x r.x
	proc	N/A	Nov 14, 2005, 3:59:45 AM	d r.x r.x r.x
	root	N/A	Nov 28, 2005, 11:01:40 AM	d rwx

The following table describes the actions necessary to access directories, files, and file and directory attributes from the Directory List page.

Table 10-2 *Directory List Page Tasks and Procedures*

Tasks	Procedures
Browse to a mount point, volume, directory, or local partition	Click the <i>link_for_the_mount_point, volume, directory, or local partition</i> under the <i>Name</i> column.
Move down the directory tree	Click the <i>directory_name</i> link.
Move up the directory tree	Click the <i>double_dots</i> (..) link.
Re-sort the list by name, size, or date and time.	Click the <i>column heading</i> that has a <i>Sort</i> icon ▼ next to it. The default sort for this listing is by the directory or file name.
View or change the attributes of a directory	Click the <i>Attributes</i> link. For information, see Section 10.2.1, “Viewing or Changing File or Directory Attributes,” on page 80 .
View the size of a directory or file.	The <i>Size</i> column for a directory lists the size of all files and subdirectories in that directory.

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

- [Section 10.2.1, “Viewing or Changing File or Directory Attributes,” on page 80](#)
- [Section 10.2.2, “Viewing Details about Directories and Performing Actions on Them,” on page 81](#)
- [Section 10.2.3, “Uploading a File to the Server,” on page 81](#)
- [Section 10.2.4, “Downloading a File from the Server to a Local Workstation,” on page 82](#)
- [Section 10.2.5, “Searching for Text in Files,” on page 82](#)
- [Section 10.2.6, “Viewing the Details of a File and Performing Specific Actions,” on page 82](#)
- [Section 10.2.7, “Viewing Individual Files,” on page 83](#)


10.2.1 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 81](#) and [“Viewing the Details of a File and Performing Specific Actions” on page 82](#).

IMPORTANT: To set directory and file attributes for files on the NSS file system, go to *Manage NCP Services > Manage Shares*, then 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 11 SP2: File Systems Management Guide*.

10.2.2 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

Type the required information in the field next to the option, then click its button.

Delete Directory and Contents	
Rename Directory	<input type="text" value="/home"/>
Create Subdirectory	<input type="text"/>
Create Symbolic Link	<input type="text"/>

10.2.3 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*.

10.2.4 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.

10.2.5 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.

10.2.6 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*.

A screenshot of a user interface showing file management options. At the top, there are three buttons: 'Edit', 'Delete', and 'Rename', followed by a text input field containing the path '/home/test/emacs'. Below these, there are two more buttons: 'Create Hard Link' and 'Create Symbolic Link', each followed by an empty text input field.

10.2.7 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 10.2.4, “Downloading a File from the Server to a Local Workstation,” on page 82](#).

10.3 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 10-3 Example Partition Information Page

Partition Information			
major	minor	#block	name
3	0	39121488	hda
3	1	2096451	hda1
3	2	4096575	hda2
3	3	1	hda3
3	5	1052226	hda5
3	6	31872928	hda6

11 Managing Linux

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 11-1 *Manage Linux Section Tasks, Links, and Pages*

Task	Link	Page Displayed	For More Info, See
Access VNC Console screens	<i>VNC Consoles</i>	VNC Consoles Screens	“Accessing VNC Consoles” on page 85
View Kernel Modules Information	<i>View Kernel Modules</i>	Kernel Module Listing	“Viewing Kernel Modules” on page 88
View Memory Information and turn swapping on and off.	<i>View Memory Information</i>	View Memory Config	“Viewing Memory Information” on page 88
Shut down and restart the host	<i>Down/Restart</i>	Down/Reset Options	“Shutting Down and Restarting the Host” on page 90
Manage packages	<i>View Package Information</i>	Package Information	“Managing Packages” on page 90
Manage processes	<i>View Process Information</i>	Process Information	“Managing Processes” on page 92
Schedule cron jobs to run	Schedule Task	Schedule Task	“Scheduling cron Jobs to Run on the Server” on page 94

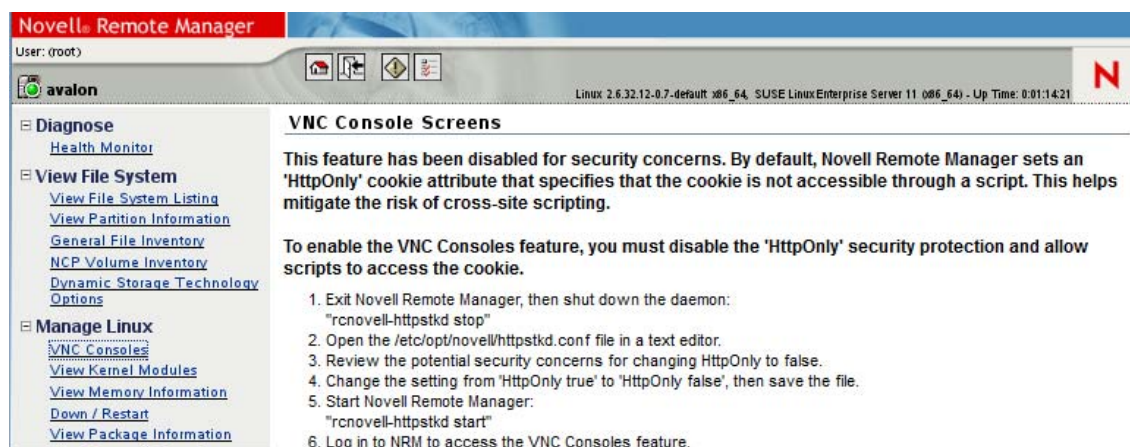
11.1 Accessing VNC Consoles

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 178](#).

- 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*.
 - 1d 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 178](#).



- 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.

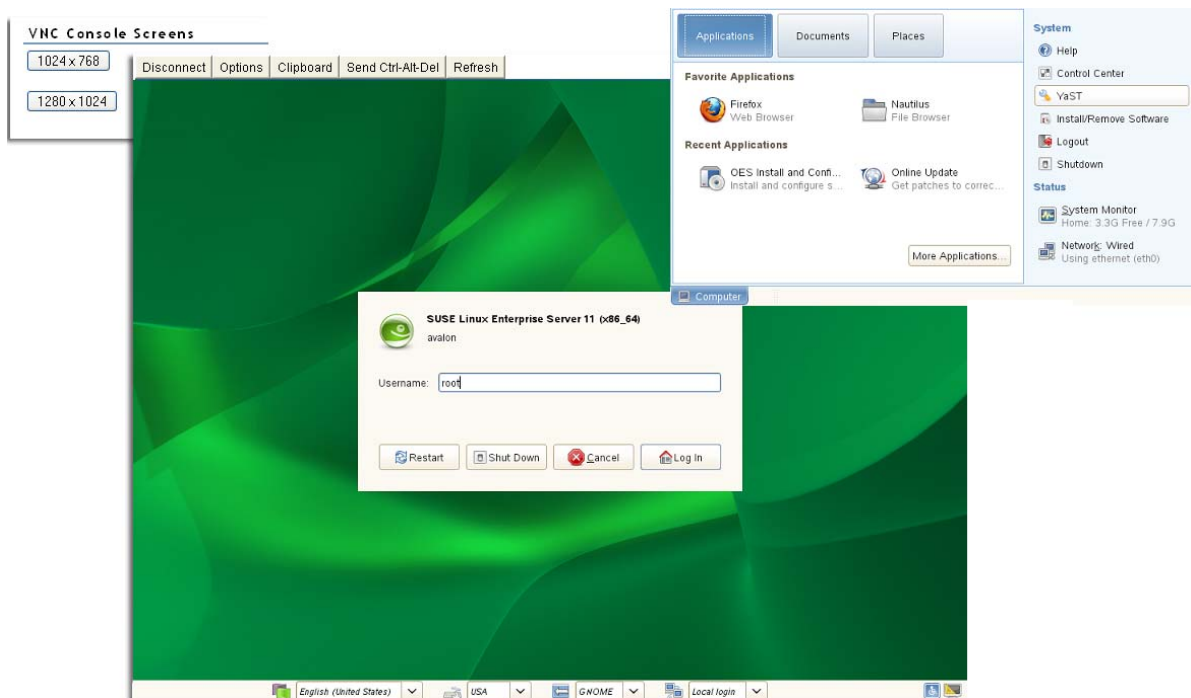
Table 11-2 VNC Console Page Tasks and Procedures

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

Figure 11-1 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 11-1 Example Access of YaST through NRM VNC Console Screens Linux on a GNOME Desktop.



11.2 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.

Figure 11-2 Example Kernel Module Listing Page

Kernel Module Listing



Kernel Module Information				
Name	Memory	Use Count	Module Users/Configuration Info	Live
ncpfs	57760	1		0xfad76000
edd	9368	0		0xfacc5000
joydev	10304	0		0xfacc1000
sg	35744	0		0xfad5b000
st	39452	0		0xfad50000
sr_mod	16292	0		0xfacbc000
ide_cd	36740	0		0xfad46000
cdrom	37148	2	sr_mod ide_cd	0xfad3b000
nvrnm	8456	0		0xfac84000
snd_seq_oss	31360	0		0xfacee000
snd_seq_midi_event	7680	1	snd_seq_oss	0xfac6a000
snd_seq	55312	4	snd_seq_oss snd_seq_midi_event	0xfacdf000

11.3 Viewing Memory Information

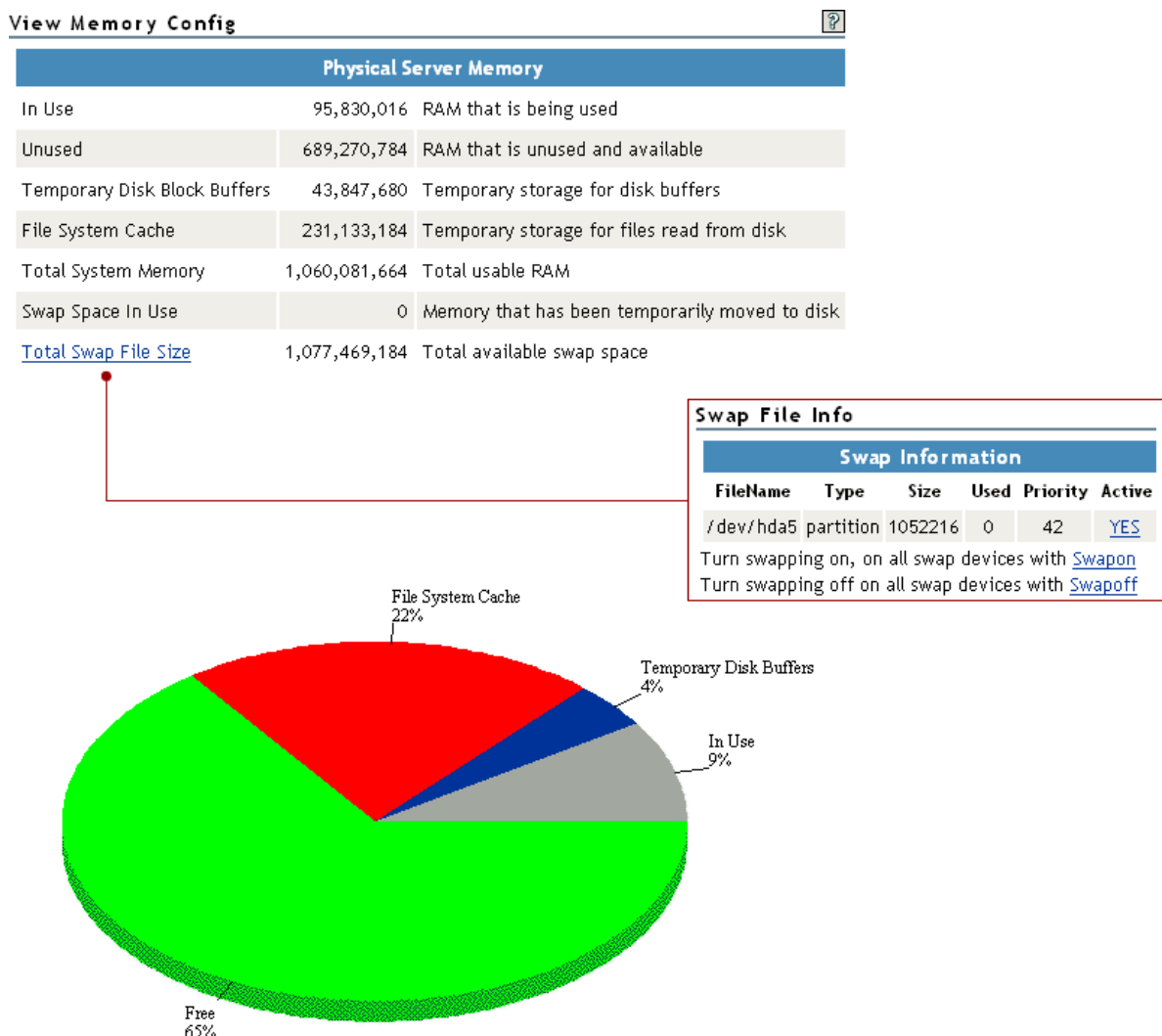
Clicking the *View Memory Information* link in the navigation frame displays the View Memory Config page. On this page you can view the following information about the memory in the server. The amount values are shown in bytes.

- ♦ Used and unused amounts of physical memory
- ♦ Amount of memory in buffer cache
- ♦ Amount of memory used by the file system cache
This value is determined by subtracting the SwapCache from the PageCache (disk cache) amounts.
- ♦ Amount of total memory that can be used by the system.
This value is determined by subtracting the physical RAM from the kernel binary code.
- ♦ Amount of swap space in use and available.

- ♦ The *Total Swap File Size* link goes to a Swap File Information page that provides a very quick snapshot of every swap file name, type of swap space, and total and used sizes (in kilobytes) on the server including the following information:
 - ♦ The Priority column is useful when multiple swap files are in use and some of them are preferred over others, such as if they are on faster hard disks. The lower the priority, the more likely the swap file will be used.
 - ♦ The Active column shows a *Yes* or *No* status, indicating whether the Swap file is active or not. Clicking the link toggles swapping on or off for the listed device.
 - ♦ Two additional links turn swapping on or off for all devices.
- If you add a swap file to a device, you need to add an entry to the `/etc/fstab` file to make the `swapon` or `swapoff` links work correctly.

This information is also in the `/proc/swaps` file.

Figure 11-3 Example View Memory Config Page



11.4 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 11-3 *Down/Reset Options Page Options and Actions*

Option	Action
<i>Down</i>	Forces the host to shut down immediately.
<i>Reset</i>	Forces the host to shut down immediately, then warm boots the computer.

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

11.5 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 11-4 Example Package Information Page

Package Information ?				
Package Information		Install	Search (case sensitive)	
Name ▼	Group ▼	Version	Release	Vendor ▼
3ddiag	System/Base	0.716	116.1	SUSE Linux AG, Nuernberg, Germany
aaa_base	System/Fhs	9	29.20	SUSE Linux AG, Nuernberg, Germany
aaa_base_novell	System/Fhs	0.0.1	3	(none)
aaa_skel	System/Fhs	2004.6.8	0.2	SUSE Linux AG, Nuernberg, Germany
aalib	System/Libraries	1.4.0	279.1	SUSE Linux AG, Nuernberg, Germany
acl	System/Filesystems	2.2.21	54.4	SUSE Linux AG, Nuernberg, Germany
acroread	Productivity/Publishing/PDF	5.010	4.2	SUSE Linux AG, Nuernberg, Germany
alsa	System/Libraries	1.0.3	41.3	SUSE Linux AG, Nuernberg, Germany
apache2	Productivity/Networking/Web/Servers	2.0.49	27.21	SUSE Linux AG, Nuernberg, Germany
apache2-jakarta-tomcat-connectors	Productivity/Networking/Web/Frontends	5.0.19	29.1	SUSE Linux AG, Nuernberg, Germany
apache2-worker	Productivity/Networking/Web/Servers	2.0.49	27.21	SUSE Linux AG, Nuernberg, Germany
arts	Productivity/Multimedia/Sound/Players	1.2.1	35.4	SUSE Linux AG, Nuernberg, Germany
ash	System/Shells	0.4.18	56.1	SUSE Linux AG, Nuernberg, Germany
at	System/Daemons	3.1.8	898.1	SUSE Linux AG, Nuernberg, Germany
atk	System/Libraries	1.4.1	128.1	SUSE Linux AG, Nuernberg, Germany
attr	System/Filesystems	2.4.16	1.2	SUSE Linux AG, Nuernberg, Germany
audiofile	System/Libraries	0.2.5	37.1	SUSE Linux AG, Nuernberg, Germany
autofs	System/Daemons	3.1.7	900.1	SUSE Linux AG, Nuernberg, Germany
autovast2	System/YaST	2.9.52	0.2	SUSE Linux AG, Nuernberg, Germany

On the View Package Information page and subsequent pages, you can perform these tasks using the following procedures:

Table 11-4 View Package Information Page Tasks and Procedures

Tasks	Procedures
Sort the listed packages by name, group, or vendor	<p>Click the <i>Sort</i> icon ▼ at the top of the applicable column.</p> <p>The default sort is by name.</p>
View more detailed information about an installed package	Click the link for the applicable package under the <i>Name</i> column.
Remove an installed package	<ol style="list-style-type: none"> 1. Click the <i>link for the package</i> under the <i>Name</i> column. 2. Click <i>Remove</i>.
Install a new package that you have downloaded to the host	<ol style="list-style-type: none"> 1. Click <i>Install</i>. 2. Browse to the location where you uploaded the package to. The browse starts at the root of the host. 3. Click <i>Install</i>. <p>The selected package's file path is transferred to the <i>RPM File Path</i> field on the Package Installation page.</p> <p>When the <i>Install</i> button is clicked on the View Package Information page, Novell Remote Manager attempts to install the specified RPM file using the Linux RPM utility.</p>

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

Figure 11-5 Detailed Information Page for the 3ddiag Example Package

3ddiag

Name : 3ddiag

Version : 0.716

Release : 116.1

Install date: Wed Jan 26 08:59:05 2005

Group : System/Base

Size : 47076

Signature : DSA/SHA1, Thu Jul 1 06:47:54 2004, Key ID a84edae89c800aca

Packager : http://www.suse.de/feedback

Summary : A Tool to Verify the 3D Configuration

Description :
With 3Ddiag you can verify the 3D configuration.

Relocations: (not relocatable)

Vendor: SuSE Linux AG, Nuernberg, Germany

Build Date: Thu Jul 1 06:46:41 2004

Build Host: millikan.suse.de

Source RPM: 3ddiag-0.716-116.1.src.rpm

License: GPL

Authors:

Stefan Dirsch
Distribution: SuSE SLES-9 (i586)

Remove

11.6 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 11-5 Process Information Page Tasks and Procedures

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


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 11-6 on page 93 describes the parameters reported for each process.
























Table 11-6 Process Information

Parameter	Description
Name	The process name.
Owner	The process owner; the user who started the process.
ID (Status)	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 < 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).
CPU Usage %	The task's share of the CPU time since the last screen update, expressed as a percentage of total CPU time per processor.
Priority	The priority of the task.
Run Time	The total CPU time the task has used since it started.
Physical Memory	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.
Virtual Memory	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.

Figure 11-6 Example Process Information Page

Process Information


Stop Refresh

Process Information							
Name 	Owner 	ID  (Status)	CPU Usage % 	Priority 	Run Time 	Physical Memory (%) 	Virtual Memory 
 aio/0	root	10 (Sleep)	0.0%	9	0:00.00	0 (0.0%)	0
 cron	root	4429 (Sleep)	0.0%	16	0:00.00	708608 (0.0%)	1617920
 events/0	root	3 (Sleep)	0.0%	5	0:00.11	0 (0.0%)	0
 httpstkd	root	2612 (Sleep)	0.0%	16	0:10.87	6807552 (0.0%)	135266304
 hwscand	root	3140 (Sleep)	0.0%	15	0:00.00	430080 (0.0%)	1441792
 init	root	1 (Sleep)	0.0%	16	0:05.01	249856 (0.0%)	602112
 kacpid	root	4 (Sleep)	0.0%	13	0:00.00	0 (0.0%)	0
 kblockd/0	root	5 (Sleep)	0.0%	5	0:00.00	0 (0.0%)	0
 khelper	root	6 (Sleep)	0.0%	5	0:00.00	0 (0.0%)	0
 khubd	root	2290 (Sleep)	0.0%	15	0:00.00	0 (0.0%)	0
 klogd	root	2541 (Sleep)	0.0%	16	0:00.00	606208 (0.0%)	1544192
 kseriod	root	678 (Sleep)	0.0%	25	0:00.00	0 (0.0%)	0
 ksoftirqd/0	root	2 (Sleep)	0.0%	34	0:00.00	0 (0.0%)	0
 kswapd0	root	9 (Sleep)	0.0%	25	0:00.00	0 (0.0%)	0
 master	root	4264 (Sleep)	0.0%	17	0:00.00	1478656 (0.0%)	4276224

11.7 Scheduling cron Jobs to Run on the Server

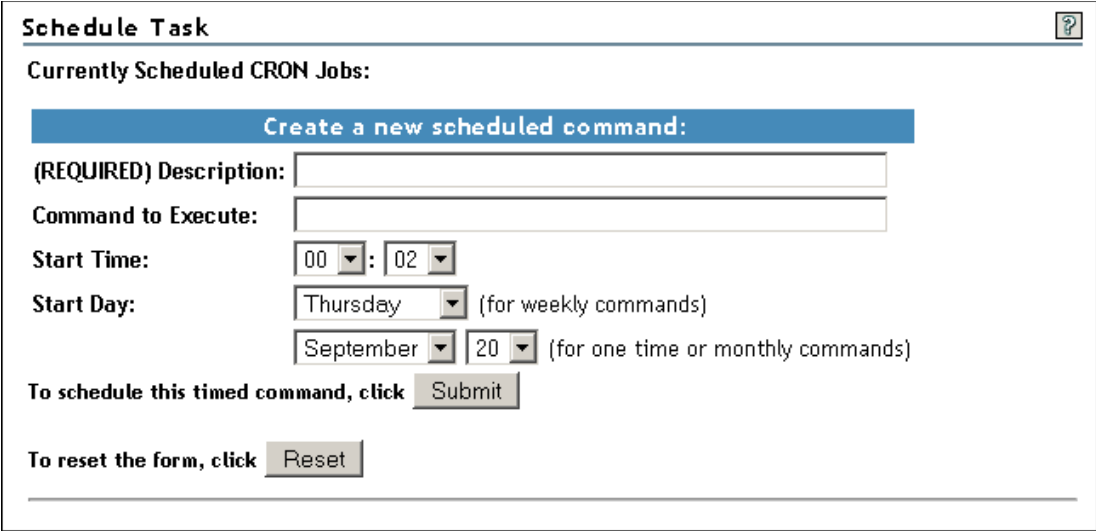
Rather than entering commands on the command line to run a cron job at a specific time, you can use a form on the Schedule Task page to schedule cron jobs—that is, to execute commands or scripts (groups of commands) automatically at a specified time/date—that you want to run at this server. Any cron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

Figure 11-7 Schedule Task Page for Scheduling Cron Jobs



The screenshot shows a web form titled "Schedule Task" with a help icon in the top right corner. Below the title is a section labeled "Currently Scheduled CRON Jobs:". A blue button labeled "Create a new scheduled command:" is positioned above the input fields. The form includes the following fields and controls:

- (REQUIRED) Description:** A text input field.
- Command to Execute:** A text input field.
- Start Time:** Two dropdown menus for hours (00) and minutes (02).
- Start Day:** A dropdown menu set to "Thursday" with the text "(for weekly commands)" to its right.
- Start Date:** Two dropdown menus for the month (September) and day (20), with the text "(for one time or monthly commands)" to their right.
- Submit:** A button labeled "Submit" preceded by the text "To schedule this timed command, click".
- Reset:** A button labeled "Reset" preceded by the text "To reset the form, click".

To create a new scheduled command:

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

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

- 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*.

12 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 12-1 *Manage Hardware Section Tasks, Links, and Pages*

Task	Link	Page Displayed	For More Info, See
View Processor information	<i>View Processors</i>	Processor Information	“Viewing Processors” on page 97
View Interrupt information	<i>Interrupt Information</i>	Interrupts	“Viewing Interrupt Information” on page 98
View memory I/O information	<i>I/O Memory Information</i>	I/O Memory Information	“Viewing I/O Memory Information” on page 99
View port I/O information	<i>I/O Port Information</i>	IO Port Information	“Viewing I/O Port Information” on page 100
View SMBIOS information	<i>SMBIOS Information</i>	SMBIOS Information	“Viewing SMBIOS Information” on page 101


12.1 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 12-1 *Example Processor Information Page*

Processor Information 	
processor : 0	
vendor_id	GenuineIntel
cpu family	15
model	3
model name	Intel(R)
Pentium(R)	134555524
4 CPU 3.00GHz	3.000000.3
stepping	
cpu MHz	2993 .171
flags	fpu vme de pse tsc msr pae mce cx8 sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe pn1 monitor ds

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.

12.2 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 12-2 *Interrupts Page*

Category	Information Displayed
Interrupt	Interrupt number or name of an interrupt that might be generated.
CPU <i>number</i>	Number of interrupts that have occurred on a given processor.
Route-Trigger Method	How the interrupt is being delivered to the processor and the method of interrupting the processor.
Device	Name of the device driver that is generating the interrupt.

Figure 12-2 Example Interrupt Information Page

Interrupts			
Interrupt Information			
Interrupt	CPU0	Route-Trigger Method	Device
0:	4,084,188	XT-PIC	timer
1:	1,132	XT-PIC	i8042
2:	0	XT-PIC	cascade
5:	0	XT-PIC	ehci_hcd
8:	2	XT-PIC	rtc
9:	93,026	XT-PIC	acpi, libata, eth0, uhci_hcd
10:	0	XT-PIC	uhci_hcd, Intel ICH5
11:	0	XT-PIC	uhci_hcd, uhci_hcd
12:	4,630	XT-PIC	i8042
14:	16,200	XT-PIC	ide0
15:	77	XT-PIC	ide1
NMI:	0		
LOC:	0		
ERR:	0		
MIS:	0		

12.3 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 12-3 I/O Memory Information Page

Category	Information Displayed
Memory Address	I/O memory range that a given device is using.
Device Description	A description of the device that is using a given I/O memory range.

Figure 12-3 Example I/O Memory Information Page

I/O Memory Information	
Memory Address	Device Description
00000000-0009ffff	System RAM
000a0000-000bffff	Video RAM area
000d1000-000d3fff	Extension ROM
000f0000-000fffff	System ROM
00100000-3ff73fff	System RAM
00100000-002ffe16	Kernel code
002ffe17-003afdf	Kernel data
3ff74000-3ff75fff	ACPI Non-volatile Storage
3ff76000-3ff96fff	ACPI Tables
3ff97000-3ffffff	reserved
e8000000-efffffff	0000:00:00.0
f0000000-f7ffffff	PCI Bus #01
f0000000-f7ffffff	0000:01:00.0
f0000000-f1ffffff	vesafb
fcfe0000-fcffffff	0000:02:0c.0

12.4 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 12-4 IO Port Information Page

Category	Information Displayed
IO Address	Shows the I/O port range that a given device is using.
Device Description	Shows the name of the device that is using a given I/O port range.

Figure 12-4 Example I/O Port Information Page

I/O Port Information

I/O Port Information	
IO Address	Device Description
0000-001f	dma1
0020-0021	pic1
0040-005f	timer
0060-006f	keyboard
0070-0077	rtc
0080-008f	dma page reg
00a0-00a1	pic2
00c0-00df	dma2
00f0-00ff	fpu
0170-0177	ide1
01f0-01f7	ide0
02f8-02ff	serial
0376-0376	ide1
03c0-03df	vesafb
03f6-03f6	ide0

12.5 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 12-5](#).

Figure 12-5 Example SMBIOS and BIOS Information Pages

SMBIOS Information

Information Type

- [BIOS Information](#)
- [System Information](#)
- [Base Board Information](#)
- [System Enclosure or Chassis](#)
- [Processor Information](#)
- [Cache Information](#)
- [Port Connector Information](#)
- [System Slots](#)
- [On Board Device Information](#)
- [OEM Strings](#)
- [BIOS Language Information](#)
- [System Event Log](#)
- [Physical Memory Array](#)
- [Memory Device](#)
- [Memory Array Mapped Address](#)
- [Memory Device Mapped Address](#)
- [Hardware Security](#)
- [System Power Controls](#)
- [Voltage Probe](#)

BIOS Information

Name	Value
BIOS Vendor	Dell Computer Corporation
BIOS Version	A04
BIOS Release Date	01/15/2004
BIOS Characteristics	PCI is supported
	Plug and Play is supported
	APM is supported
	BIOS is Upgradeable (Flash)
	BIOS shadowing is allowed
	ESCD support is available
	Boot from CD is supported
	Selectable Boot is supported
	EDD (Enhanced Disk Drive) Specification is supported
	Int 13h - Japanese Floppy for Toshiba 1.2 MB (3.5", 360 RPM) is supported
	Int 5h, Print Screen Service is supported
	Int 9h, 8042 Keyboard services are supported
	Int 14h, Serial Services are supported
	Int 17h, Printer Services are supported
BIOS Characteristics Extension Byte 1	ACPI supported
	USB Legacy is supported

13 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 13-1 *Use Group Operations Tasks, Links, and Pages*

Task	Link	Page Displayed	For More Information
Access an existing group	<i>Select Group</i>	Select Group	“Accessing an Existing Group” on page 109
Build and configure a new monitoring group	<i>Configure New Group</i>	Group Monitoring Operations	“Building and Configuring a Monitoring Group” on page 104
Change an existing group	<i>Select Group</i>	Select Group	“Changing an Existing Group” on page 109
Define or edit Group Monitoring types	<i>NRM Health Types</i>	Novell Remote Manager Health Monitoring Engine (NRM Health Types)	“Defining or Editing Group Monitoring Types” on page 113
Delete an existing group	<i>Select Group</i>	Select Group	“Deleting an Existing Group” on page 110
Scan the network for items to monitor on the network.	<i>Configure New Group > right-click > click Network Discovery</i>	Network Discovery	“Discovering Items on the Network to Monitor” on page 114
Generate and view server reports	<i>Configure New Group > right-click > click Save Group</i>	Group Monitoring Operations	“Generating and Viewing Server Reports” on page 110
Save a new group	<i>Configure New Group > right-click > click Save Group</i>	Save Group	“Saving a Group” on page 108
View group operations monitored items	<i>View Monitored Items</i>	Novell Remote Manager Health Monitoring Engine - Monitored Items	“Viewing Monitored Items” on page 111
View group operations defined NRM health types	<i>NRM Health Types</i>	Novell Remote Manager Health Monitoring Engine - NRM Health Types	“Viewing Group Monitoring Types” on page 112

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

1. [Building and Configuring a Monitoring Group \(page 104\)](#).
2. (Optional) [Saving a Group \(page 108\)](#).

You only need to perform this step if you want to use the group at a later time.

3. [Generating and Viewing Server Reports \(page 110\)](#).

The monitoring operations start immediately. Other tasks, such as running reports require additional steps.

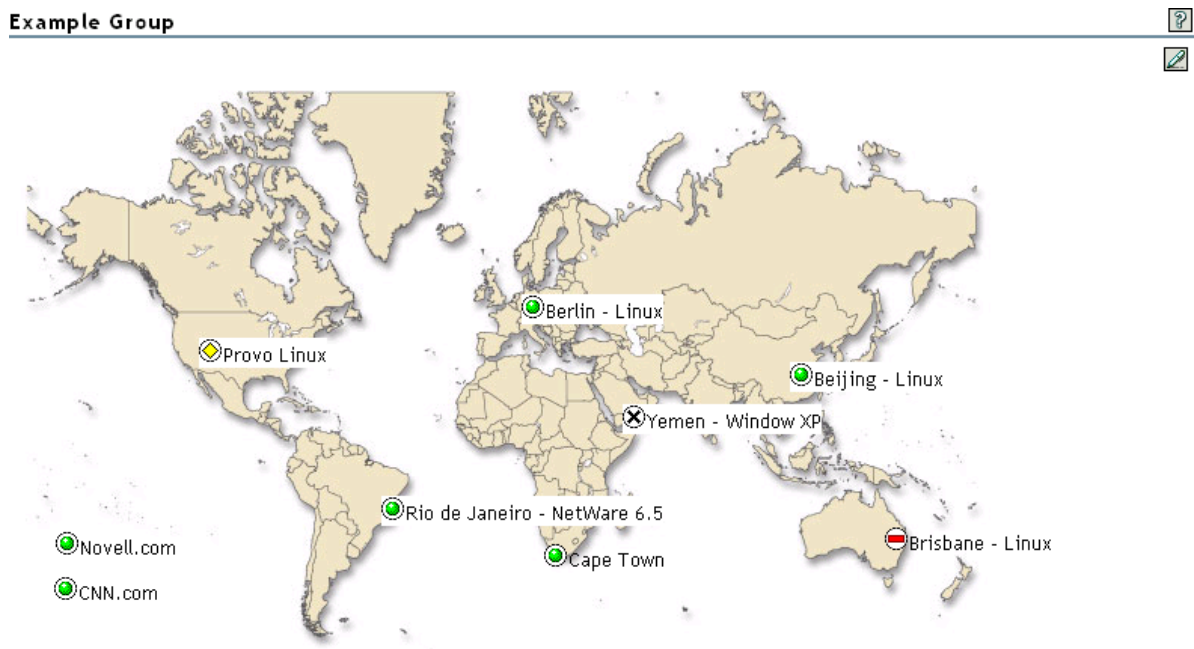
4. (Conditional) [Accessing an Existing Group \(page 109\)](#).

13.1 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 13-1 NRM Server Health Example Group

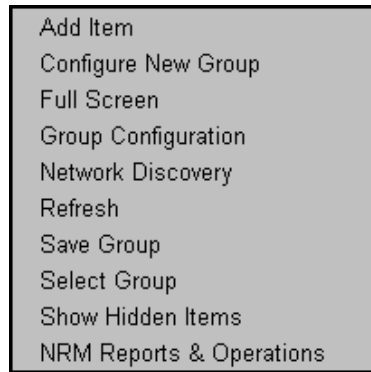


To build and configure a new monitor group:

- 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:



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.

Add New Monitor Item



Monitoring Item Configuration			
Name	<input type="text"/>	Monitoring Type	NRM Health Monitor <input type="button" value="v"/>
Item Address/URL	<input type="text"/>	Port	8008
Hide Normal Status	<input type="checkbox"/>		
Text Color	Default <input type="button" value="v"/>	Text Background Color	Default <input type="button" value="v"/>
Use single sign on NRM credentials	<input type="checkbox"/>		
User Name	<input type="text"/>	Password	* <input type="text"/>
<input type="button" value="Add"/>		<input type="button" value="Cancel"/>	

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.

Option	Details
<i>Monitoring Type</i>	<p>Specify one of the following types:</p> <ul style="list-style-type: none"> ♦ Label: Text information to use as a label on the group monitor display. Lets you identify each group specifically as needed. ♦ LDAP Directory Root Search: 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. ♦ NRM Group: Shows the health status of a group of servers. Lets you access the specific health page for each server in the group. ♦ NRM Health Monitor: Shows the health status of each server in the group. Lets you access the specific health page for each server in the group. ♦ Ping (ICMP): Shows the response when sending ping requests to the specified DNS name or IP address. ♦ TCP/IP Port Query: 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. ♦ Web page: 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 <code>www.novell.com</code>, but not <code>www.novell.com/support</code>. If you specify a subdirectory, the DNS name cannot be resolved, and a Can't Connect health status is reported.
<i>Name</i>	Provide a descriptive name for the item.
<i>Item Address/URL</i>	<p>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.</p> <p>The address can be an IP address or DNS name.</p> <p>Do not specify the HTTP:// portion of a URL.</p>
<i>Port</i>	The default is provided. You can type a different port to use.
<i>Use Single Sign on NRM Credentials</i>	<p>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.</p> <p>When deselected, enter the credential necessary to access the item in the User Name and Password fields.</p>
<i>Hide Normal Status</i>	<p>When selected, only items that are in an abnormal state are displayed.</p> <p>If you want to monitor all statuses, leave the check box deselected.</p>

Option	Details
<i>Text Color</i>	Black is the default. You can select any other color from the drop-down list.
<i>Text Background Color</i>	Clear is the default. You can select any other color in the drop-down list.

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 113](#).

- 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
?

Display Options	E-mail Options
Monitor Page Title <input style="width: 80%;" type="text"/>	Suspect Server Health E-mail Notification <input type="checkbox"/>
Background Graphic <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">NRMDefaultGroupMap.JPG ▼</div>	First notification wait period <div style="border: 1px solid #ccc; width: 40px; text-align: center;">0</div> Minutes
Refresh Rate <div style="border: 1px solid #ccc; width: 40px; text-align: center;">30</div> Seconds	Additional notification wait period <div style="border: 1px solid #ccc; width: 40px; text-align: center;">0</div> Minutes
	Critical Server Health E-mail Notification <input type="checkbox"/>
	First notification wait period <div style="border: 1px solid #ccc; width: 40px; text-align: center;">0</div> Minutes
	Additional notification wait period <div style="border: 1px solid #ccc; width: 40px; text-align: center;">0</div> Minutes

Option	Description
<i>Display</i>	<p>The display options let you control the following:</p> <ul style="list-style-type: none"> ♦ Monitor Page Title: Specify a title to be shown at the top of the monitor page in the header area when the page is built. ♦ Refresh Rate: Specify the number of seconds between status queries to the server. ♦ Background Graphic: 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. <p>If you want to add a customized graphic, add it to the <code>/opt/novell/nrm/NRMGroupMaps</code> directory.</p>
<i>Email</i>	<p>The email notification options control how and when email notifications are sent when the server health changes. Email notifications are sent to the addresses in the mail notification list using the mail servers set in the <code>/etc/opt/novell/httpstkd.conf</code> file.</p> <p>IMPORTANT: The email function is supported only on OES 11 SP1 and earlier.</p>

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 108](#).

13.2 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.

13.2.1 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.

13.2.2 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*.

13.3 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*.

13.4 Changing an Existing Group

After accessing an existing group (see [“Accessing an Existing Group” on page 109](#)), you might want to change it using one of the following procedures.

Table 13-2 *Changing an Existing Group Tasks and Procedures*

If you want to	Then
Change the configuration of an existing group.	<ol style="list-style-type: none">1. Select the group.2. Right-click the page, then click <i>Group Configuration</i>.3. Make the desired changes in the Group Operations Configuration form.4. Click <i>Apply</i>.5. Save the group. (See “Saving a Group” on page 108.)
See the details of the server health or the monitoring type.	<ol style="list-style-type: none">1. Select the group.2. Select the item you want to see the details for.3. Double-click the <i>Health Status</i> icon.

If you want to	Then
Edit an existing item in the group.	<ol style="list-style-type: none"> 1. Select the group. 2. Select the item you want to edit. 3. Right-click the selected item. 4. Click <i>Edit</i>.
Delete a server or monitor item from a group.	<ol style="list-style-type: none"> 1. Select the group. 2. Select the item you want to delete. 3. Right-click the selected item. 4. Click <i>Delete</i>.
Change the display to a full screen in your browser window.	<ol style="list-style-type: none"> 1. Select the group. 2. Right-click the page. 3. Click <i>Full Screen</i> 4. When you are finished viewing the group, close the browser window.

13.5 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*.

13.6 Generating and Viewing Server Reports

Running Server Comparison reports on a group of servers can help you in 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 110.

13.6.1 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 104 or [“Accessing an Existing Group”](#) on page 109.
- 2 Right-click the customized Group page.
- 3 Click *NRM Reports & Operation*.

Novell Remote Manager Server Information

Reports

Operations



Compare Server Up Times

NRM Servers

OES-Linux-s2

OES-Linux-s1

4 Click *Compare Server Up Times*.

A report similar to the following is returned.

Server Up Time Report

Server	Up Time
OES-Linux-s2	16 days 06 hours 05 minutes 46 seconds
OES-Linux-s1	14 days 22 hours 58 minutes 08 seconds



Server has been up less than one hour.



Server has been up less than one day.

13.7 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*.

Figure 13-2 Monitored Items

Novell Remote Manager Health Monitoring Engine

Monitored Items

Item Name	Type	Address	Last Check Time	Monitoring Start Time
avalon	NRM Agent	127.0.0.1:8008	Mon Jan 6 14:42:35 2014	Mon Jan 6 14:42:35 2014

Reset Item List

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 11 SP2 servers, see [“Viewing the Overall Server Health Status” on page 46](#)
- For OES 11 SP1 and earlier servers, see [“Overall Server Health Status” on page 71](#)

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

Table 13-3 *Health Monitoring Engine Monitored Items*

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

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.

13.8 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/NRMGroupHealthInfo` file.

Figure 13-3 The Default NRM Health Monitoring Engine - NRM Health Types Content Definitions

Novell Remote Manager Health Monitoring Engine

17

Health type defines used for Group Operations health monitoring on this machine.

NRM Health Types				
Health Type	Type String	Platform	Health Test	Default Port
NRM Health Monitor	NRM	All	NRM Health State	8008
NRM Item Health States				
	Icon	Value	Return Value	Item Click
		1	HEALTH_STATUS_GREEN	NRM Health Page
		3	HEALTH_STATUS_YELLOW	NRM Health Page
		4	HEALTH_STATUS_UNKNOWN	NRM Health Page
		5	HEALTH_STATUS_RED	NRM Health Page
		7	HEALTH_STATUS_CANT_CONNECT	NRM Health Page
Health Type	Type String	Platform	Health Test	Default Port
Label	LABEL	All	n/a	
Health Type	Type String	Platform	Health Test	Default Port
NRM Group	GROUP	All	Group Items Health	
NRM Group Health States				
	Icon	Value	Return Value	Item Click
		1	HEALTH_STATUS_GREEN	Expand Group
		3	HEALTH_STATUS_YELLOW	Expand Group
		4	HEALTH_STATUS_UNKNOWN	Expand Group
		5	HEALTH_STATUS_RED	Expand Group
		7	HEALTH_STATUS_CANT_CONNECT	Expand Group
Health Type	Type String	Platform	Health Test	Default Port
Ping(CMP)	PING	Linux	ping -c1 -W1 %ITEM_ADDR grep "bytes from" 1>/dev/null	
PING Health States				
	Icon	Value	Return Value	Item Click
		0	HEALTH_STATUS_UP	ping -c4 %ITEM_ADDR
		Not 0	HEALTH_STATUS_CANT_CONNECT	ping -c4 -W1 %ITEM_ADDR
Health Type	Type String	Platform	Health Test	Default Port
Web Page	HTTP	Linux	wget --tries=1 --output-document=/dev/null %ITEM_ADDR:%ITEM_PORT 2>/dev/null	80
HTTP Health States				
	Icon	Value	Return Value	Item Click
		0	HEALTH_STATUS_UP	http://%ITEM_ADDR:%ITEM_PORT wget --tries=1 --output-document=/dev/null %ITEM_ADDR:%ITEM_PORT 2
		Not 0	HEALTH_STATUS_CANT_CONNECT	
Health Type	Type String	Platform	Health Test	Default Port
LDAP Directory Root Search	LDAP	Linux	ldapsearch -h "%ITEM_ADDR" -x "(objectclass=Organization)" 1>/dev/null	
LDAP Health States				
	Icon	Value	Return Value	Item Click
		0	HEALTH_STATUS_UP	ldapsearch -h "%ITEM_ADDR" -x "(objectclass=Organization)"
		Not 0	HEALTH_STATUS_DOWN	ldapsearch -h "%ITEM_ADDR" -x "(objectclass=Organization)"
Health Type	Type String	Platform	Health Test	Default Port
TCP/IP Port Query	TCP_Open	Linux	nmmap -sT -p %ITEM_PORT --max_rtt_timeout 2000 %ITEM_ADDR grep "1 host up"	80
TCP_Open Health States				
	Icon	Value	Return Value	Item Click
		0	HEALTH_STATUS_UP	nmmap -sT -p %ITEM_PORT --max_rtt_timeout 2000 %ITEM_ADDR
		Not 0	HEALTH_STATUS_DOWN	nmmap -sT -p %ITEM_PORT --max_rtt_timeout 2000 %ITEM_ADDR

13.9 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.

```

<NRM_Health_Item_Definition>
  <Type_Name>PING</Type_Name>
  <Display_Name>Ping(ICMP)</Display_Name>
  <Platform>Linux</Platform>
  <Health_Test>
    <Command_Line>
      ping -c1 -W1 %ITEM_ADDR | grep "bytes from" 1>/dev/null
    </Command_Line>
    <Result>
      <Value>0</Value>
      <Result_Icon>/sys/login/NRMcanping.gif</Result_Icon>
      <Return_Value>HEALTH_STATUS_UP</Return_Value>
      <Click_Command>ping -c4 %ITEM_ADDR</Click_Command>
    </Result>
    <Result>
      <!Value>0</!Value>
      <Return_Value>HEALTH_STATUS_CANT_CONNECT</Return_Value>
      <Click_Command>ping -c4 -W1 %ITEM_ADDR</Click_Command>
    </Result>
  </Health_Test>
</NRM_Health_Item_Definition>

```

13.10 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:

NetWork Discovery


Network Scan Parameters

DNS Name/IP Address
Subnet Mask

Select a Network Discovery Method

Scan available Hosts(ping/ICMP Echo)	<input type="button" value="Subnet Scan"/>
Scan for Web Servers(port 80)	<input type="button" value="Web Server Scan"/>
Scan for LDAP Servers(port 389)	<input type="button" value="LDAP Server Scan"/>
Scan for Novell Remote Manager Servers(port 8008/8009)	<input type="button" value="NRM Agent Scan"/>
Scan for Services(user supplied port)	<input type="button" value="Service Scan"/> port: <input type="text"/>

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.

Task	Procedure
Scan the network for hosts that are responding to ICMP Echo Requests in the network within a specified subnet.	<ol style="list-style-type: none">1. Accept the default IP address or DNS name and subnet mask information or change it.2. Click <i>Subnet Scan</i>.
Scan the network for hosts with port 80 open and listening for connections (Web Servers) within a specified subnet.	<ol style="list-style-type: none">1. Accept the default IP address or DNS name and subnet mask information or change it.2. Click <i>Web Server Scan</i>.
Scan the network for hosts with port 389 open and listening for connections (LDAP Servers) within a specified subnet.	<ol style="list-style-type: none">1. Accept the default IP address or DNS name and subnet mask information or change it.2. Click <i>LDAP Server Scan</i>.
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.	<ol style="list-style-type: none">1. Accept the default IP address or DNS name and subnet mask information or change it.2. Click <i>NRM Agent Scan</i>.
Scan the network for hosts with <i>user_defined_port</i> open and listening within a specified subnet.	<ol style="list-style-type: none">1. Accept the default IP address or DNS name and subnet mask information or change it.2. Click <i>Service Scan</i>.

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:

Task	Procedure
See more information about the scanned host.	<ol style="list-style-type: none">1. Click the <i>Web Service More Info</i> 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.	<ol style="list-style-type: none">1. Click the <i>Add Item to Group</i> icon  for the applicable host on the Network Discovery page.2. Complete the required information on the Add New Monitor Item page, then click <i>Add</i>. <p>Most of the information is completed by default.</p>

14 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 Novell Open Enterprise Server (OES) 11 SP2, see the [OES 11 SP2: NCP Server for Linux Administration Guide](#).

For information about using and managing NSS volumes on OES 11 SP2, see the [OES 11 SP2: 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 14-1 Links for Managing NCP Services

Link	Page Displayed	For More Information
<i>View Inventory Reports</i>	NCP Inventory Reports <ul style="list-style-type: none">♦ Generate report♦ Display last report	Section 14.3, “Generating Inventories for Directories or NCP Volumes,” on page 133
<i>View Trustee Reports</i>	NCP Trustee Reports <ul style="list-style-type: none">♦ Generate report♦ Display last report	Section 14.6, “Generating and Viewing NCP Trustee Reports for NSS Volumes,” on page 140
<i>Manage Shares</i>	NCP Shares <ul style="list-style-type: none">♦ Active shares listing for NSS volumes and NCP volumes♦ Information about shares, including open files♦ Create new share♦ Delete existing share♦ NCP/NSS bindings	“Managing NCP Volumes” in the OES 11 SP2: NCP Server for Linux Administration Guide
<i>Manage Server</i>	NCP Manage Server <ul style="list-style-type: none">♦ Server parameters for NCP Server♦ Global policy parameters for Dynamic Storage Technology	“Managing NCP Server” in the OES 11 SP2: NCP Server for Linux Administration Guide

Link	Page Displayed	For More Information
<i>Manage Connections</i>	Connections <ul style="list-style-type: none"> ◆ Connection information (statistics) ◆ Broadcast message to everyone ◆ Connection listing ◆ Detailed information about a connection, including open files 	“Managing Connections for NCP Volumes and NSS Volumes” in the OES 11 SP2: NCP Server for Linux Administration Guide
<i>View Logs</i>	NCP System Logs <ul style="list-style-type: none"> ◆ Logs <ul style="list-style-type: none"> ◆ ncpserv.log ◆ ncp2nss.log ◆ Audit logs <ul style="list-style-type: none"> ◆ ncpserv.audit.log ◆ ncp2nss.audit.log ◆ SYS.audit.log ◆ <volume_name>.audit.log 	“Log Files” in the OES 11 SP2: NCP Server for Linux Administration Guide
<i>View Statistics</i>	NCP Statistical Information <ul style="list-style-type: none"> ◆ Server information ◆ Server statistics 	“NCP Server Statistics” in the OES 11 SP2: NCP Server for Linux Administration Guide
<i>View Diagnostic Information</i>	NCP Diagnostic Information <ul style="list-style-type: none"> ◆ NCP engine ◆ NSS interface daemon 	Chapter 8, “Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2),” on page 45 Chapter 9, “Diagnosing Problems Using Health Monitor (OES 11 SP1),” on page 69

From these pages you can perform the following tasks:

- ◆ [Section 14.1, “Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux,” on page 119](#)
- ◆ [Section 14.2, “Browsing NSS Volumes and Performing Actions on Them,” on page 124](#)
- ◆ [Section 14.3, “Generating Inventories for Directories or NCP Volumes,” on page 133](#)
- ◆ [Section 14.4, “Generating a Custom Inventory Report from a File Inventory Report,” on page 138](#)
- ◆ [Section 14.5, “Performing Actions on Files from Custom Reports,” on page 139](#)
- ◆ [Section 14.6, “Generating and Viewing NCP Trustee Reports for NSS Volumes,” on page 140](#)

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

- ♦ [Section 14.1.1, “NCP Volumes \(NCP Shares\),” on page 119](#)
- ♦ [Section 14.1.2, “NCP Server Parameters,” on page 120](#)
- ♦ [Section 14.1.3, “NCP Server Connections,” on page 120](#)
- ♦ [Section 14.1.4, “NCP Trustee Reports,” on page 121](#)
- ♦ [Section 14.1.5, “NCP Logs and Audit Logs,” on page 121](#)
- ♦ [Section 14.1.6, “NCP Server Statistics,” on page 122](#)
- ♦ [Section 14.1.7, “NCP Server Diagnostics,” on page 122](#)
- ♦ [Section 14.1.8, “Dynamic Storage Technology,” on page 123](#)

14.1.1 NCP Volumes (NCP Shares)

[Table 14-2](#) describes the management tasks available for the *Manage NCP Services > Manage Shares* task in Novell Remote Manager for Linux.

Table 14-2 *Manage NCP Services > Manage Shares*

Subtasks	Management Tasks
Share Name link	<p>Browse files and directories.</p> <p>View and set file system attributes for files and directories on NSS volumes.</p> <p>View file information.</p> <p>View directory information.</p>
Mount/Unmount	<p>Mount NCP volumes and NSS volumes to make them available to NCP clients.</p> <p>Unmount NCP volumes and NSS volumes to make them unavailable to NCP clients.</p>
Info icon	<p>NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics.</p> <p>Open files listed for each NCP connection.</p> <p>Add a shadow volume for the NCP volume.</p> <p>For unmounted DST shadow volumes, click the <i>Info</i> icon to remove the shadow volume relationship. Removing a shadow volume removes the entry in the <code>ncpserv.conf</code> file, but does not delete the volumes that make up the shadow volume.</p>
Create new share	<p>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.</p> <p>IMPORTANT: You cannot use this method to create an NSS volume. You must use NSS tools to create and manage NSS volumes on Linux.</p>

Subtasks	Management Tasks
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.
NCP/NSS bindings	<p>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.</p> <p>Use this option for NSS volumes on clusters where the load script handles NCP mount of NSS volumes.</p> <p>Use this option for NSS volumes that you want to use as the secondary storage area in a Dynamic Storage Technology shadow volume.</p>

14.1.2 NCP Server Parameters

[Table 14-3](#) describes the management task available for the *Manage NCP Services > Manager Server* task in Novell Remote Manager for Linux.

Table 14-3 *Manage NCP Services > Manage Server*

Subtasks	Management Tasks
Server Parameter Information	<p>View NCP Server parameters for the <code>SET</code> command and their current values.</p> <p>Click the <i>Parameter Value</i> link to modify the value. For a list of parameters and their default values, see “Configuring Global NCP Server Parameters” in the <i>OES 11 SP2: NCP Server for Linux Administration Guide</i>.</p>

14.1.3 NCP Server Connections

[Table 14-4](#) describes the management tasks available for the *Manage NCP Services > Manage Connections* task in Novell Remote Manager for Linux.

Table 14-4 *Manage NCP Services > Manage Connections*

Subtasks	Management Tasks
Connection information	<p>View connection statistics.</p> <p>Clear all <i>Not Logged In</i> connections.</p>
Connection listing	<p>View a list of connections.</p> <p>Click the name link for the connection to view statistics for the connection and a list of its open files.</p> <p>Clear selected connections.</p>

Subtasks	Management Tasks
Name link for the connection	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.
Broadcast messages to everyone	Broadcast messages to all logged-in NCP users. The <code>DISABLE_BROADCAST</code> 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.

14.1.4 NCP Trustee Reports

Table 14-5 describes the management tasks available for the *Manage NCP Services > NCP Trustee Report* task in Novell Remote Manager for Linux.

Table 14-5 *Manage NCP Services > NCP Trustee Report*

Subtasks	Management Tasks
Generating an NCP Trustee report for NSS volumes	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.
Viewing a saved NCP Trustee report	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.
Emailing a saved NCP Trustee report	For OES 11 SP1 and earlier, email an NCP volume's trustee report to addresses that are configured in the <code>httpstkd.conf</code> file.

14.1.5 NCP Logs and Audit Logs

Table 14-6 describes the management tasks available for the *Manage NCP Services > View Logs* task in Novell Remote Manager for Linux.

Table 14-6 *Manage NCP Services > View Logs*

Subtasks	Management Tasks
Logs	Download and view the <code>ncpserv.log</code> and <code>ncp2nss.log</code> .

Subtasks	Management Tasks
Audit logs	<p>Download and view the following audit logs:</p> <ul style="list-style-type: none"> ◆ <code>ncpserv.audit.log</code> <p>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.</p> <ul style="list-style-type: none"> ◆ <code>ncp2nss.audit.log</code> <p>The following ncp2nss events are logged into this file:</p> <p>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.</p> <ul style="list-style-type: none"> ◆ <code>SYS.audit.log</code> ◆ <code>volumename.audit.log</code> (an audit log is listed for each NSS volume)

14.1.6 NCP Server Statistics

[Table 14-7](#) describes the management tasks available for the *Manage NCP Services > View Statistics* task in Novell Remote Manager for Linux.

Table 14-7 *Manage NCP Services > View Statistics*

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

14.1.7 NCP Server Diagnostics

[Table 14-8](#) describes the management tasks available for the *Manage NCP Services > Diagnostic Information* task in Novell Remote Manager for Linux.

Table 14-8 *Manage NCP Services > Diagnostic Information*

Subtasks	Management Tasks
NCP engine	<p>View statistics for NCP events.</p> <p>Click the <i>Process ID (PID)</i> link to view information about the currently running process.</p>

Subtasks	Management Tasks
NSS interface daemon	View statistics for NSS events. Click the <i>Process ID (PID)</i> link to view information about the currently running process.

14.1.8 Dynamic Storage Technology

Table 14-9 describes the management tasks available for the *View File Systems > Dynamic Storage Technology Options* task in Novell Remote Manager for Linux.

Table 14-9 *View File Systems > Dynamic Storage Technology Options*

Subtasks	Management Tasks
Volume information	View a list of NCP volumes and NSS volumes on the server. Click the <i>Add Shadow</i> 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.) Click the <i>Inventory</i> link next to a shadow volume to view an inventory report for both the primary and secondary volumes. Click the <i>View Log</i> link next to an NSS volume to download a copy of the audit log for the selected volume.
Add Shadow link	This option takes you to the Share Information page. Scroll down to the <i>Volume Tasks</i> area to find the <i>Add Shadow Volume</i> task. 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. WARNING: NSS volumes must already exist when you create the shadow volume. The <i>Create if not present</i> option is available for future support of NCP volumes on Linux file systems. Do not use this option for NSS volumes.
Inventory link	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).
Volume information (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 access the dialog to remove the shadow volume relationship. This removes the entry in the <code>ncpserv.conf</code> file, but does not delete the volume itself. To unmount a shadow volume, click <i>Manage NCP Services > Manage Shares</i> , then click <i>Unmount</i> option next to the shadow volume.

Subtasks	Management Tasks
Dynamic Storage Technology policies	<p>Create a new policy.</p> <p>View a list of existing policies.</p> <p>Click the <i>Policy Name</i> link to modify or delete the policy.</p>
Duplicate file resolution options	Set a global policy for how to handle duplicate files.
ShadowFS configuration	Set a global policy for whether to automatically start FUSE and Shadow File System at boot time.

14.2 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 11 SP2: NCP Server for Linux Administration Guide](#).

For detailed information about creating and managing NSS volumes, see the [OES 11 SP2: 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 11 SP2: Dynamic Storage Technology Administration Guide](#).

- ♦ [Section 14.2.1, “Viewing Information about an NSS Volume,” on page 124](#)
- ♦ [Section 14.2.2, “Viewing the Linux POSIX Details of an NSS Directory and Performing Specific Actions on It,” on page 126](#)
- ♦ [Section 14.2.3, “Viewing the Linux POSIX Details of a File and Performing Specific Actions on It,” on page 127](#)
- ♦ [Section 14.2.4, “Browsing an NSS Volume and Setting Rights and File System Attributes on Directories and Files,” on page 128](#)
- ♦ [Section 14.2.5, “Salvaging and Purging Deleted Files on an NSS Volume,” on page 132](#)
- ♦ [Section 14.2.6, “Purging a Deleted NSS Volume,” on page 132](#)
- ♦ [Section 14.2.7, “Viewing Open File Information for an NSS Volume,” on page 133](#)

14.2.1 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 (i) to go to the volume's Share Information page.

VOLD Share Information 

Information	
Description	Value
File system path	/media/nss/VOLD
File system shadow path	n/a
Loaded name spaces	DOS LONG
File system type	NSS
NCP volume ID	2
Status	mounted online salvageable user quotas directory quotas
Sector Size	512
Sectors per Cluster	8
Capacity	496.52 MB
Used space	592 KB
Advanced Information	View

[Open File Information](#)

[Salvageable File List](#)

Volume tasks

Available Actions

[Add Shadow volume](#)

[Purge Volume](#)

[Perform Inventory](#)

[Share Management Home](#)

- 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.)

Local cache	
Parameter	Value
trustee count	0
cached files	2
evicted files	0
cached folders	5
cache retrieved	19
cache retrieved locked	0
Pool name	NSS POOL_D
Pool attributes	NSS 0x13
GUID	NSS e3b410a4-f2fa-01e1-80-00-0c8f5f6d1d22

- ◆ 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.)

14.2.2 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
- ♦ Last accessed time
- ♦ Information change time
- ♦ Linux POSIX read/write/execute directory 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:

A screenshot showing four buttons for directory management: 'Delete Directory and Contents', 'Rename Directory', 'Create Subdirectory', and 'Create Symbolic Link'. Each button is paired with an input field. The 'Rename Directory' input field contains the text '/media/nss/VOLD/dir1/dir2'. The other input fields are empty.

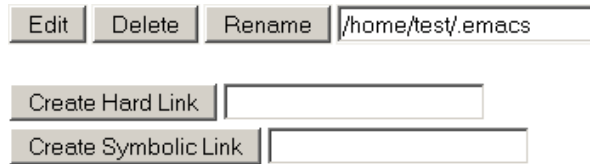
- ♦ **Delete Directory and Its Contents:** Click this option to delete the selected directory and the subdirectories and files in it.
- ♦ **Rename Directory:** Specify the full Linux path to the directory, including the new directory name, then click *Rename Directory*.
- ♦ **Create Subdirectory:** Specify the name of the new subdirectory, then click *Create Subdirectory*.
- ♦ **Create Symbolic Link:** Specify the name for the symbolic link, then click *Create Symbolic Link*.

14.2.3 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:



The image shows a user interface for file management. At the top, there are three buttons: 'Edit', 'Delete', and 'Rename'. To the right of the 'Rename' button is a text input field containing the path '/home/test/emacs'. Below these buttons, there are two more buttons: 'Create Hard Link' and 'Create Symbolic Link'. Each of these buttons is followed by an empty text input field for specifying a path.

- ♦ **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*.

14.2.4 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 14.3, “Generating Inventories for Directories or NCP Volumes,”](#) on page 133.


- 5 Click a directory's *Directory Information* icon  to view information about the directory. You can also create subdirectories.

Figure 14-1

VOLD:/dir1

[\[Back to directory listing for: /VOLD/dir1\]](#)

Directory entry information:

Owner	.avalon.novell
Creation date and time	Mon Nov 14 13:57:12 2011
Effective rights	SRWCEMFA
Inherited rights filter	SRWCEMFA

Salvageable files: None

Create Subdirectory New name

- ♦ Owner
 - ♦ 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.


VOLD:/dir1

Folder Attributes	Description
<input type="checkbox"/> System	If checked, this indicates a system file or folder.
<input type="checkbox"/> Hidden	If checked, this indicates that this file or folder is excluded from normal directory searches.
<input type="checkbox"/> Archive	If checked, this indicates that the file or folder needs to be archived.
<input type="checkbox"/> Immediate Purge	If checked, this indicates that when this file or folder or the folder contents are deleted and are unrecoverable.
<input type="checkbox"/> Don't Compress	If checked, this indicates that this file or the contents of the folder cannot be compressed..
<input type="checkbox"/> Don't Migrate	If checked, this indicates that this file or folder cannot be migrated to near line storage..
<input type="checkbox"/> Delete Inhibit:	If checked, this indicates that this file or folder cannot be deleted.
<input type="checkbox"/> Rename Inhibit:	If checked, this indicates that this file or folder name cannot be renamed.
<input type="checkbox"/> Immediate Compress	If checked, this indicates that this file or the folder contents will be scheduled for compression..

- ♦ 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 11 SP2: 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

[\[Back to directory listing for: /VOLD\]](#)

File information

Owner	.admin.novell
Last modified date and time	Fri Nov 11 18:43:40 2011
Creation date and time	Fri Nov 11 18:43:40 2011
Last archived date and time	Fri Nov 30 00:00:00 1979
Effective rights	SRWCEMFA
Inherited rights filter	SRWCEMFA
Disk space in use	4,845,095 Bytes

Delete File

- ♦ 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.

VOLD:/SLES-deployment_en.pdf

File Attributes	Description
<input type="checkbox"/> System	If checked, this indicates a system file or folder.
<input type="checkbox"/> Hidden	If checked, this indicates that this file or folder is excluded from normal directory searches.
<input type="checkbox"/> Read Only	If checked, this indicates that this file cannot be deleted or modified..
<input checked="" type="checkbox"/> Archive	If checked, this indicates that the file or folder needs to be archived.
<input type="checkbox"/> Immediate Purge	If checked, this indicates that when this file or folder or the folder contents are deleted and are unrecoverable.
<input type="checkbox"/> Don't Compress	If checked, this indicates that this file or the contents of the folder cannot be compressed..
<input type="checkbox"/> Don't Migrate	If checked, this indicates that this file or folder cannot be migrated to near line storage..
<input type="checkbox"/> Delete Inhibit:	If checked, this indicates that this file or folder cannot be deleted.
<input type="checkbox"/> Rename Inhibit:	If checked, this indicates that this file or folder name cannot be renamed.
<input type="checkbox"/> Immediate Compress	If checked, this indicates that this file or the folder contents will be scheduled for compression..
<input type="checkbox"/> Shareable	If checked, this indicates that this file may be used by multiple users at the same time..
<input type="checkbox"/> Don't SubAlloc	If checked, this indicates that this file may not utilize sub-allocation for space saving..
<input type="checkbox"/> Execute Only	If checked, this indicates that this file may only be excuted as a program, no modifications will be allowed to the file.
<input type="checkbox"/> Transactional	If checked, this indicates that Transactional tracking of data will enabled.
<input type="checkbox"/> Copy Inhibit	If checked, this indicates that this file may not be copied.
OK Reset	

- ◆ 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 11 SP2: File Systems Management Guide*.

14.2.5 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 11 SP2: 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

[\[Back to directory listing for: /VOLD\]](#)

Purge all files

Salvageable files

Salvage	Purge	Name	Size	Last modified date and time	Deletor
Salvage	Purge	SLES-installquick_en.pdf	4446726	Fri Nov 11 18:45:06 2011	.admin.novell

- 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.

14.2.6 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 11 SP2: NSS File System Administration Guide for Linux*.

- 1 In Novell Remote Manager, select *Manage NCP Service > 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*.

14.2.7 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 11 SP2: NCP Server for Linux Administration Guide*.
 - ♦ User name
 - ♦ Open file list

14.3 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.

IMPORTANT: To view the graphical displays in the inventory report, Java must be installed on the computer you use to access Novell Remote Manager. The browser must have Java and Javascript enabled.

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.

This section includes the following tasks:

- ♦ [Section 14.3.1, "Generating a File Inventory Report," on page 134](#)
- ♦ [Section 14.3.2, "Generating an NCP Volume Inventory Report," on page 135](#)
- ♦ [Section 14.3.3, "Viewing a Saved NCP Inventory Report," on page 137](#)
- ♦ [Section 14.3.4, "Emailing a Saved NCP Inventory Report \(OES 11 SP1\)," on page 137](#)

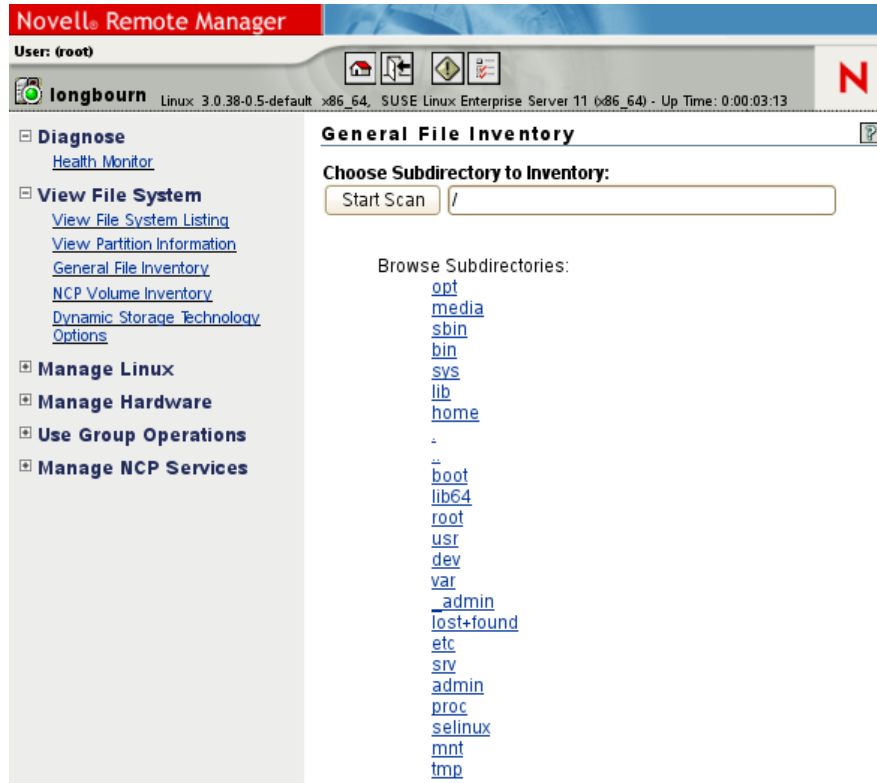
14.3.1 Generating a File Inventory Report

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

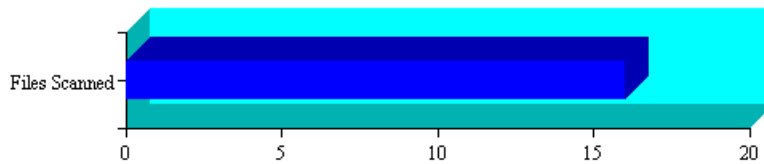
Browse Subdirectories:

..
..

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



Inventory Report for: /home/test

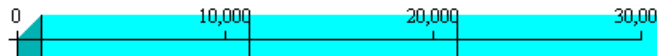
[File type profiles](#)
[File owner profiles](#)
[Last modified profiles](#)
[Last accessed profiles](#)
[Change time profiles](#)
[File size profiles](#)
[Links to specific reports](#)
[Custom Directory Tree Scan](#)

Key Statistics	Totals
Total Subdirectories:	6
Total Files:	16
Space In Use:	0 MB
File Types:	4
Soft Link Files:	0
Soft Link Subdirectories:	0

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 138.

14.3.2 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.

Diagnose

View File System

Manage Linux

Manage Hardware

Use Group Operations

Manage NCP Services

View Inventory Reports

NCP Inventory Reports

Volume	View Last Report	Generate Report	eMail Report
VOL1	Display	Create	Send
VOL_SH1	Display	Create	Send
SYS	Display	Create	Send

- ♦ 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.

▢ **Diagnose**

[Health Monitor](#)

▢ **View File System**

[View File System Listing](#)

[View Partition Information](#)

[General File Inventory](#)

[NCP Volume Inventory](#)

[Dynamic Storage Technology Options](#)

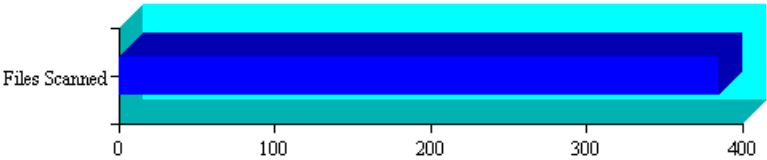
Volume Inventory ?

NCP Volumes Available for Inventory	
Volume	Mount Point
SYS	(/usr/novell/sys)
NCPVOL	(/home)
VOL_D	(/media/nss/VOL_D)
VOL_F	(/media/nss/VOL_F)

2 View the generated report.

A report similar to the following is generated:

Volume Inventory



Inventory Report for: /usr/novell/sys

[File type profiles](#)

[File owner profiles](#)

[Last modified profiles](#)

[Last accessed profiles](#)

[Change time profiles](#)

[File size profiles](#)

[Links to specific reports](#)

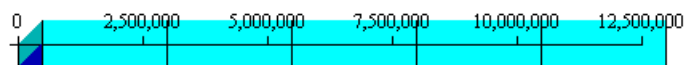
[Custom Directory Tree Scan](#)

Key Statistics	Totals
Total Subdirectories:	35
Total Files:	385
Space In Use:	21 MB
File Types:	12
Soft Link Files:	0
Soft Link Subdirectories:	0

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 138.


14.3.3 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.

<div><div>⊞ Diagnose</div><div>⊞ View File System</div><div>⊞ Manage Linux</div><div>⊞ Manage Hardware</div><div>⊞ Use Group Operations</div><div>⊞ Manage NCP Services</div><div><div>View Inventory Reports</div></div></div>	NCP Inventory Reports 			
	Volume	View Last Report	Generate Report	eMail Report
	VOL1	Display	Create	Send
	VOL_SH1	Display	Create	Send
	SYS	Display	Create	Send

14.3.4 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 176.

IMPORTANT: The Novell Remote Manager email notification system is not available beginning in OES 11 SP2.

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.

14.4 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 134](#).
- 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:

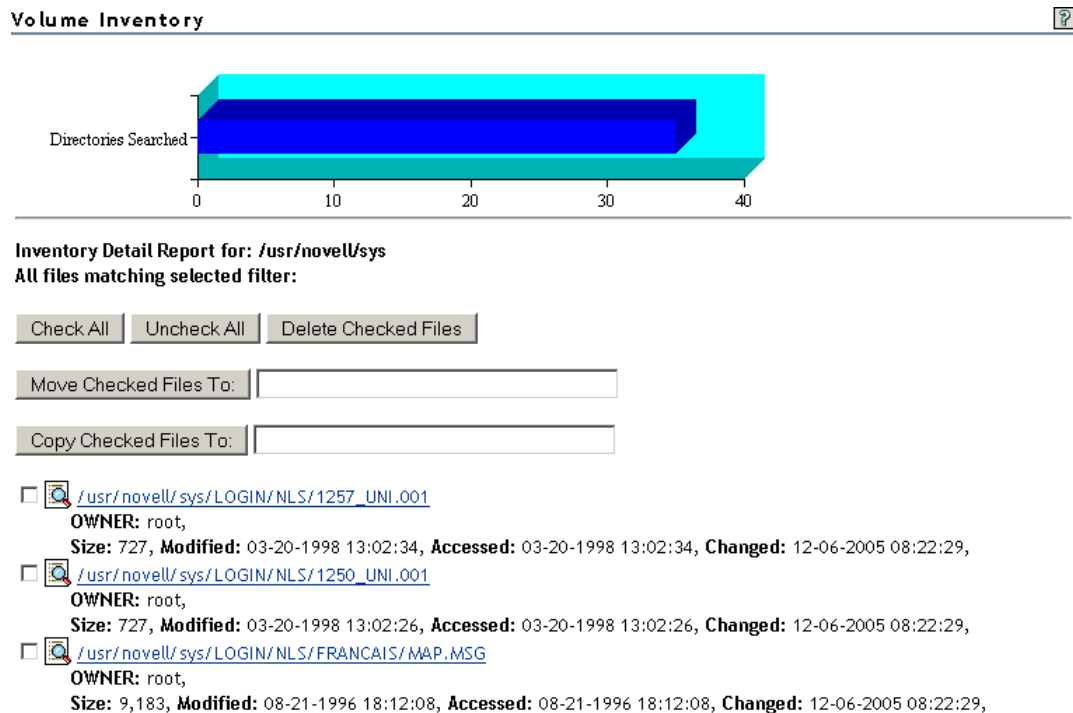
- ☐ Within Last Day
- ☐ 1 Day - 1 Week
- ☐ 1 Week - 2 Weeks
- ☐ 2 Weeks - 1 Month
- ☐ 1 Month - 2 Months
- ☐ 2 Months - 4 Months
- ☐ 4 Months - 6 Months
- ☐ 6 Months - 1 Year
- ☐ 1 Year - 2 Years
- ☐ More than 2 Years

File Size Restriction:

- ☐ Less than 1KB
- ☐ 1 KB - 4 KB
- ☐ 4 KB - 16 KB
- ☐ 16 KB - 64 KB
- ☐ 64 KB - 256 KB
- ☐ 256 KB - 1 MB
- ☐ 1 MB - 4 MB
- ☐ 4 MB - 16 MB
- ☐ 16 MB - 64 MB
- ☐ 64 MB - 256 MB
- ☐ More than 256 MB

- 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.
- 6 Click *Start Scan*.
A page similar to the following is returned:



14.5 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 14.5.1, “Moving Selected Files,” on page 139](#)
- ♦ [Section 14.5.2, “Copying Selected Files,” on page 140](#)
- ♦ [Section 14.5.3, “Deleting Selected Files,” on page 140](#)
- ♦ [Section 14.5.4, “Opening or Downloading a File,” on page 140](#)
- ♦ [Section 14.5.5, “Managing Individual Files,” on page 140](#)

14.5.1 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.

14.5.2 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.
The target path must be to a location on the same volume.
- 3 Click the *Copy Checked File To* button.


14.5.3 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.

14.5.4 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*.

14.5.5 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.

Edit	Delete	Rename	<input type="text" value="/home/test/.emacs"/>
Create Hard Link	<input type="text"/>		
Create Symbolic Link	<input type="text"/>		

14.6 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 14.6.1, “Generating an NCP Trustee Report,” on page 141](#)
- ♦ [Section 14.6.2, “Viewing a Saved NCP Trustee Report,” on page 141](#)
- ♦ [Section 14.6.3, “Emailing a Saved NCP Trustee Report \(OES 11 SP1\),” on page 141](#)


14.6.1 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.

NCP Trustee Reports 			
Volume	View Last Report	Generate Report	Email Report
V3	Display	Create	Send
V2	Display	Create	Send
V1	Display	Create	Send

- 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: <code>/media/nss/V1</code>	
Shadow Volume Tree: <code>/media/nss/V1SHADOW</code>	
Report generated on Fri Mar 16 18:28:14 2012	
/media/nss/V1/folderjim	
Rights: <code>_RWCEMFA</code>	User / Group <code>.CN=nonlumuser2.O=novell.T=TULIP.</code>
Elapsed Time(seconds): 14	

14.6.2 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.

14.6.3 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 176.

IMPORTANT: The Novell Remote Manager email notification system is not available beginning in OES 11 SP2.

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.

15 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 Novell Open Enterprise Server (OES) 11 SP2, see the [OES 11 SP2: Dynamic Storage Technology Administration Guide](#).

For information about using and managing NSS volumes on OES 11 SP2, see the [OES 11 SP2: 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 15-1 *Links for Dynamic Storage Technology Options*

Link	Actions
<i>View File Systems > Dynamic Storage Technology Options > Volume Information</i>	<div>Volume Share Information</div> <ul style="list-style-type: none">♦ View file system shadow path♦ Add shadow volume <div>See “Adding a Shadow to the Primary NSS Volume (Linking the NSS Volumes)” in the OES 11 SP2: Dynamic Storage Technology Administration Guide.</div>
<i>View File Systems > Dynamic Storage Technology Options > Shadow Status</i>	<ul style="list-style-type: none">♦ Shadowed♦ Add Shadow <div>See “Adding a Shadow to the Primary NSS Volume (Linking the NSS Volumes)” in the OES 11 SP2: Dynamic Storage Technology Administration Guide.</div>
<i>View File Systems > Dynamic Storage Technology Options > Inventory</i>	<div>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 11 SP2: Dynamic Storage Technology Administration Guide.</div>

Link	Actions
<i>View File Systems > Dynamic Storage Technology Options > Dynamic Storage Technology Policies</i>	<ul style="list-style-type: none"> ♦ 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 <i>Delete</i>. <p>See “Viewing DST Policies and Policy Status” in the <i>OES 11 SP2: Dynamic Storage Technology Administration Guide</i>.</p>
<i>View File Systems > Dynamic Storage Technology Options > Create a new policy</i>	See “Creating and Managing Policies for Shadow Volumes” in the <i>OES 11 SP2: Dynamic Storage Technology Administration Guide</i> .
<i>View File Systems > Dynamic Storage Technology Options > Stop all running policies</i>	See “Stopping a Running Policy” in the <i>OES 11 SP2: Dynamic Storage Technology Administration Guide</i> .
<i>View File Systems > Dynamic Storage Technology Options > Duplicate file resolution options</i>	<ul style="list-style-type: none"> ♦ Broadcast conflict message to user ♦ Action to be taken <ul style="list-style-type: none"> ♦ 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 <p>See “Resolving Instances of Duplicate Files” in the <i>OES 11 SP2: Dynamic Storage Technology Administration Guide</i>.</p>
<i>View File Systems > Dynamic Storage Technology Options > Loading Shadow FS</i>	See “Using ShadowFS to Provide a Merged View for Novell Samba Users” in the <i>OES 11 SP2: Dynamic Storage Technology Administration Guide</i> .
<i>Manage NCP Services > Manage Shares > NCP Shares</i>	<p>NCP Shares</p> <ul style="list-style-type: none"> ♦ NCP/NSS bindings ♦ Volume Information > Volume Tasks > Add Shadow Volume ♦ Unmount > Volume Information > Volume Tasks > Remove Shadow <p>For information about adding and removing shadow volume pairs, see “Creating and Managing DST Shadow Volumes for NSS Volumes” in the <i>OES 11 SP2: Dynamic Storage Technology Administration Guide</i>.</p>

Link	Actions
<i>Manage NCP Services > Manage Server</i>	<p>NCP Manage Server</p> <ul style="list-style-type: none"> ♦ Global policy parameters for Dynamic Storage Technology <p> DUPLICATE_SHADOW_FILE_ACTION DUPLICATE_SHADOW_FILE_BROADCAST REPLICATE_PRIMARY_TREE_TO_SHADOW SHIFT_ACCESSED_SHADOW_FILES SHIFT_DAYS_SINCE_LAST_ACCESS SHIFT_MODIFIED_SHADOW_FILES </p> <p>For more information about how these settings affect shadow volume pairs on the server, see “Configuring DST Global Policies” in the <i>OES 11 SP2: Dynamic Storage Technology Administration Guide</i>.</p>

16 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) 11 SP2, see the [OES 11 SP2: Novell CIFS for Linux Administration Guide](#).

For information about using and managing NSS volumes on OES 11 SP2, see the [OES 11 SP2: NSS File System Administration Guide for Linux](#).

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

Table 16-1 Links for Manage CIFS Services

Link	Page Displayed
Manage Connections	CIFS Connections
View Logs	CIFS System Logs <ul style="list-style-type: none">♦ libnrm2cifs.log♦ cifs.log
Manage Open Files	CIFS Open File Management <ul style="list-style-type: none">♦ Connection information (statistics)♦ Connection listing♦ Detailed information about a connection, including open files

From these pages you can perform the following tasks:

- ♦ [Section 16.1, “Managing CIFS Connections,” on page 148](#)
- ♦ [Section 16.2, “Viewing Log Information,” on page 148](#)
- ♦ [Section 16.3, “Managing Open Files,” on page 149](#)

16.1 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 16-2 CIFS Connection Parameters

Parameter	Description
Access mode	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.
DD	Indicates that the right to delete or rename the file is denied for all other connections.
Desired access	Specifies the access modes that the client has requested.
DR	Indicates that the right to read data from the file is denied.
DW	Indicates that the right to write data into the file is denied.
ND	Indicates that the right to delete or rename the file is denied for this connection.
RD	Indicates that the right to read data from the file is granted.
Shared access	Specifies the sharing modes that the client has requested; that is, how the file should be shared with other users.
WR	Indicates that the right to write data into the file is granted.

- 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, and login details for the connection.
 - ♦ **View Connection Information:** Click the connection name to view more details for a specific connection.

16.2 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.

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 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.

17 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 Novell Open Enterprise Server (OES) 11 SP2, see the [OES 11 SP2: Novell AFP for Linux Administration Guide](#).

For information about using and managing NSS volumes on OES 11 SP2, see the [OES 11 SP2: NSS File System Administration Guide for Linux](#).

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

Table 17-1 Links for Manage AFP Services

Link	Page Displayed
Manage Connections	AFP Connections
View Logs	AFP System Logs <ul style="list-style-type: none">♦ <code>afptcp.log</code>♦ <code>libnrm2afp.log</code>
Manage Open Files	AFP Open File Management <ul style="list-style-type: none">♦ Connection information (statistics)♦ Connection listing♦ Detailed information about a connection, including open files

From these pages you can perform the following tasks:

- ♦ [Section 17.1, “Managing AFP Connections,” on page 152](#)
- ♦ [Section 17.2, “Viewing Log Information,” on page 152](#)
- ♦ [Section 17.3, “Managing Open Files,” on page 153](#)

17.1 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 17-2 *AFP Connections Parameters*

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

- 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.

17.2 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.

3 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.

17.3 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.

18 Tasks Quick Reference

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 18-1 Task Quick Reference List

Tasks	Link in Navigation frame or Other Location	For More Information
Build a group for monitoring	<i>Use Group Operations > Configure New Group</i>	Building and Configuring a Monitoring Group (page 104)
Cron job, schedule	<i>Manage Linux > Schedule Task</i>	“Scheduling cron Jobs to Run on the Server” on page 94
Directory, change attributes of	<i>View File System > View File System Listing</i>	Viewing Details about Directories and Performing Actions on Them (page 81)
Directory, edit	<i>View File System > View File System Listing</i>	Viewing Details about Directories and Performing Actions on Them (page 81)
Directory, delete	<i>View File System > View File System Listing</i>	Viewing Details about Directories and Performing Actions on Them (page 81)
Directory, rename	<i>View File System > View File System Listing</i>	Viewing Details about Directories and Performing Actions on Them (page 81)
Directory, view detailed information about	<i>View File System > View File System Listing</i>	Viewing Details about Directories and Performing Actions on Them (page 81)
File, change attributes of	<i>View File System > View File System Listing</i>	Viewing the Details of a File and Performing Specific Actions (page 82)
File, download	<i>View File System > View File System Listing</i>	Downloading a File from the Server to a Local Workstation (page 82)
File, edit	<i>View File System > View File System Listing</i>	Viewing the Details of a File and Performing Specific Actions (page 82)
File, delete	<i>View File System > View File System Listing</i>	Viewing the Details of a File and Performing Specific Actions (page 82)

Tasks	Link in Navigation frame or Other Location	For More Information
File, rename	<i>View File System > View File System Listing</i>	Viewing the Details of a File and Performing Specific Actions (page 82)
Files, search for text in	<i>View File System > View File System Listing</i>	Searching for Text in Files (page 82)
File, upload	<i>View File System > View File System Listing</i>	Uploading a File to the Server (page 81)
File, view	<i>View File System > View File System Listing</i>	Viewing Individual Files (page 83)
File system, browse	<i>View File System > View File System Listing</i>	Browsing File Systems and Performing Actions on Them (page 79)
File system, perform action on	<i>View File System > View File System Listing</i>	Browsing File Systems and Performing Actions on Them (page 79)
Files, viewing details about	<i>View File System > View File System Listing</i>	Viewing the Details of a File and Performing Specific Actions (page 82)
Group operations, access an existing group	<i>Use Group Operations > Select Group</i>	Accessing an Existing Group (page 109)
Group operations, build and configure a new monitoring group	<i>Use Group Operations > Configure New Group</i>	Building and Configuring a Monitoring Group (page 104)
Group operations, change an existing group	<i>Use Group Operations > Select Group</i>	Changing an Existing Group (page 109)
Group operations, define or edit Group Monitoring types	<i>Use Group Operations > NRM Health Types</i>	Defining or Editing Group Monitoring Types (page 113)
Group operations, delete an existing group	<i>Use Group Operations > Select Group</i>	Deleting an Existing Group (page 110)
Group operations, discover items to monitor on the network.	<i>Use Group Operations > Configure New Group > right-click menu > Network Discovery</i>	Discovering Items on the Network to Monitor (page 114)
Group operations, generate and view server reports	<i>Use Group Operations > Configure New Group > right-click menu > Save Group</i>	Generating and Viewing Server Reports (page 110)
Group operations, save a new group	<i>Use Group Operations > Configure New Group > right-click menu > Save Group</i>	Saving a Group (page 108)
Group operations, view defined health types	<i>Use Group Operations > NRM Health Types</i>	Viewing Group Monitoring Types (page 112)
Group operations, view monitored items	<i>View Monitored Items</i>	Viewing Monitored Items (page 111)
Host, shut down	<i>Manage Linux > Down/Reset Options</i>	Shutting Down and Restarting the Host (page 90)

Tasks	Link in Navigation frame or Other Location	For More Information
Host, restart	<i>Manage Linux > Down/Reset Options</i>	Shutting Down and Restarting the Host (page 90)
Interrupt information, view	<i>Manage Hardware > Interrupt Information</i>	Viewing Interrupt Information (page 98)
I/O Memory information, view	<i>Manage Hardware > IO Memory Information</i>	Viewing I/O Memory Information (page 99)
IO Port information, view	<i>Manage Hardware > IO Port Information</i>	Viewing I/O Port Information (page 100)
Kernel modules, view	<i>Manage Linux > Kernel Module Listing</i>	Viewing Kernel Modules (page 88)
Memory information, view	<i>Manage Linux > View Memory Information</i>	Viewing Memory Information (page 88)
Mounted devices, perform actions on them	<i>Home icon > Info icon</i>	Viewing Mounted Devices and Performing Actions on Them (page 78)
Mounted devices, view	<i>Home icon > Info icon</i>	Viewing Mounted Devices and Performing Actions on Them (page 78)
Packages, install	<i>Manage Linux > Package Information</i>	Managing Packages (page 90)
Packages, remove	<i>Manage Linux > Package Information</i>	Managing Packages (page 90)
Packages, view information about	<i>Manage Linux > Package Information</i>	Managing Packages (page 90)
Partition information, view	<i>View File System > View Partition Information</i>	Viewing Partition Information (page 83)
Process, kill	<i>Manage Linux > Process Information</i>	Managing Processes (page 92)
Process, view information about	<i>Manage Linux > Process Information</i>	Managing Processes (page 92)
Processors, view information about	<i>Manage Hardware > View Processors</i>	Viewing Processors (page 97)
OES 11 SP2 Server health	<i>Diagnose > Server Health Values</i> <i>Diagnose > Server Health Services</i>	Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2) (page 45)
OES 11 SP2 Nagios	<i>Configuration Options > Nagios Configuration</i>	Configuring Nagios (page 53)
OES 11 SP2 Nagios user management	<i>Configuration Options > Nagios Configuration > Nagios User Management</i>	Managing Nagios Users (page 61)
OES 11 SP2 Nagios alert notification system for Ganglia and Nagios health alerts	<i>Configuration Options > Nagios Configuration</i>	Modifying the Nagios Notification Methods for Contacts (page 64)

Tasks	Link in Navigation frame or Other Location	For More Information
OES 11 SP1 Server health, configure email notification about status	<i>Health Monitor and Configuration Icon</i>	Configuring Email Notification for Server Health Status (page 74)
OES 11 SP1 Server health, configure item to monitor	<i>Diagnose > Health Monitor</i>	Configuring the Items to Monitor (page 73)
OES 11 SP1 Server health, monitor health of a specific item	<i>Diagnose > Health Monitor</i>	Monitoring Overall Server Health or the Health of a Specific Item (page 70)
OES 11 SP1 Server health, monitor overall health	<i>Diagnose > Health Monitor</i>	Monitoring Overall Server Health or the Health of a Specific Item (page 70)
OES 11 SP1 Server health, troubleshooting suspect or bad health status	<i>Diagnose > Health Monitor</i>	Troubleshooting a Suspect or Bad Health Status (page 75)
Server Group, monitor overall server health	<i>Use Group Operation > Configure New Group or Select Group</i>	Building and Configuring a Monitoring Group (page 104)
SMBIOS information, view	<i>Manage Hardware > SMBIOS Information</i>	Viewing SMBIOS Information (page 101)
Swap information, view	<i>Manage Linux > View Memory Information</i>	Viewing Memory Information (page 88)

19 Troubleshooting Novell Remote Manager

This section describes known issues and workarounds for Novell Remote Manager for Novell Open Enterprise Server 11.

- [Section 19.1, “Daemon httpstkd Is Unable to Start,” on page 159](#)
- [Section 19.2, “Error while loading shared libraries: libldapx.so.0,” on page 159](#)
- [Section 19.3, “Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 11 SP2,” on page 160](#)
- [Section 19.4, “Inventory Graphics Are Not Displayed in the Web Browser,” on page 161](#)
- [Section 19.5, “Ganglia Statistical Graphics Are Not Displayed in the Web Browser,” on page 165](#)

19.1 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
```

19.2 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:

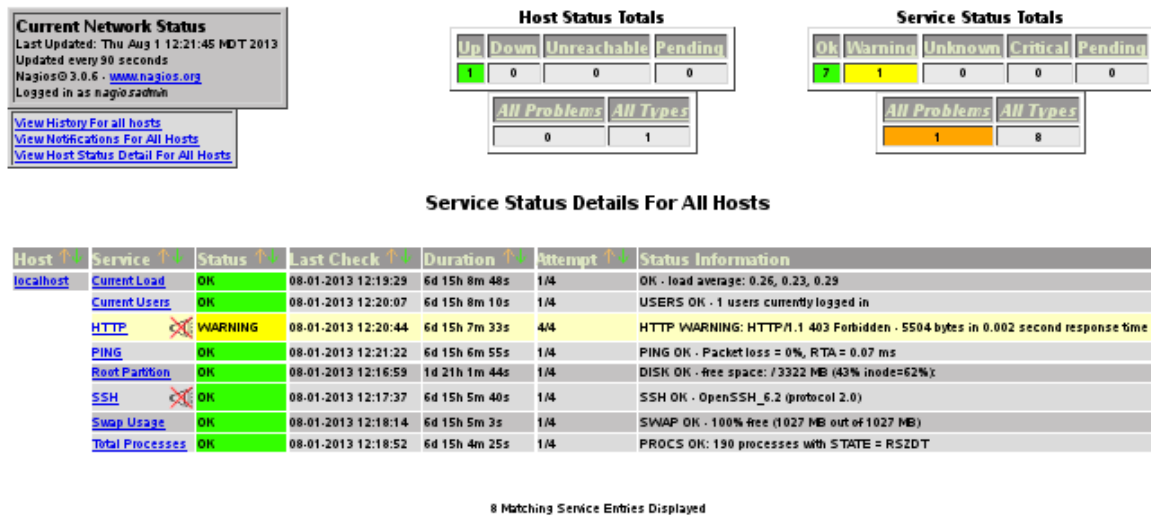
```
Starting the Novell Small Http Interface
Daemon/opt/novell/httpstkd/sbin/httpstkd: error while loading shared libraries:
libldapx.so.0: cannot open shared object file: No such file or directory
```

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.

19.3 Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 11 SP2

You might see an Apache 403 Forbidden Warning error reported in Nagios after a new installation or upgrade to OES 11 SP2.

Figure 19-1 HTTP 403 Forbidden Warning Error



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 `check_command` 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
    check_command       check_http! -e 'HTTP/1.0 200','HTTP/
1.1 200','HTTP/1.1 403 Forbidden'

    notifications_enabled 0
}
```

NOTE: If the status for any other service is yellow or red, you must modify the relevant parameters in the `localhost.cfg` file. For example, if you have 300 processes running on your cluster node, the status of Total Processes will display yellow, since the default values are set to 250 (yellow color) and 400 (red color). You can modify the values to 400 and 500 depending on your environment.


```
define service {
    use          local-service      ; Name of service template to use
    host_name    localhost
    service_description    Total Processes
    check_command    check_local_procs!400!500!RSZDT
}
```

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.

19.4 Inventory Graphics Are Not Displayed in the Web Browser

In order to view the graphical displays in the file system inventory report, Java must be installed on the machine you use to access Novell Remote Manager, and the browser must have Java and Javascript enabled.

The Java plug-in for Firefox is not installed by default on your OES server. To install the Java browser plug-in for the default installed version of Java on an OES server:

1 Close all open instances of the web browser on the server.

2 Launch YaST2 as the root user.

3 In the YaST2 menu, select *Software > Software Management*.

4 In the Software Manager dialog box, select the *Search* tab, type `java` in the search field, then click *Search*.

5 Select the Java browser plug-in for the installed version of Java.

For example, in OES 11 SP2, Java 6.0 IBM (JRE 1.6.0 IBM) is the default version of Java. The browser plug-in is the `java-1_6_0-ibm-plugin` RPM file.

6 Click *Accept*.

7 Close YaST2.

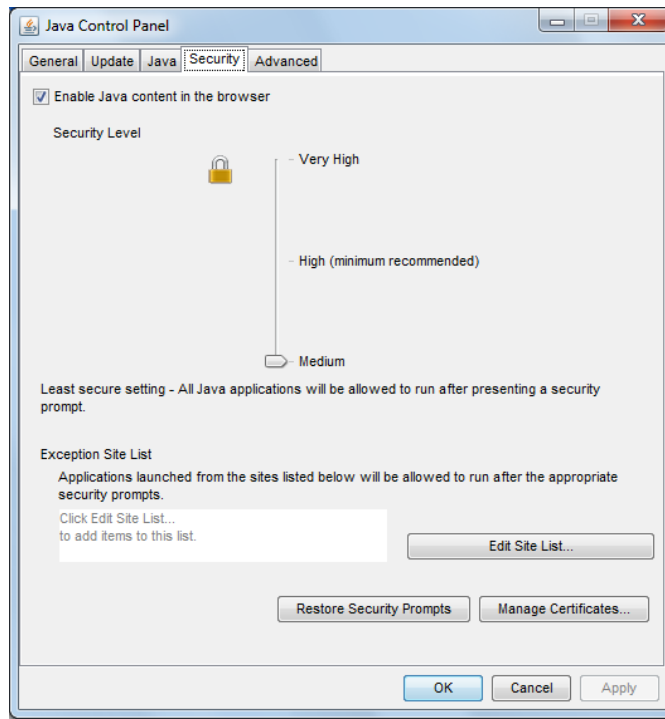
8 Verify that the server's web browser can display inventory graphics. Launch the Firefox web browser on the server, log in to Novell Remote Manager, and then create a file inventory report.

The graphics should be visible when you create a file inventory report with Novell Remote Manager. On newer versions of Java, you might get warning messages about unsigned certificates or self-signed certificates. After reviewing the certificate information, allow the graphics application to run.

In Java 7 Update 51 (Java JRE 1.7.0_51) and later, applets with self-signed or unsigned certificates are blocked by the Java default *Security* setting of *High*, or a setting of *Very High*. You can set the Java *Security* setting to *Medium* in order to allow the graphical display applet to run after presenting a security prompt. Other security warnings about unsigned certificates or self-signed certificates must also be addressed.

To modify the Java *Security* setting on a Windows computer:

- 1 Close your web browser.
- 2 Open the Java management console. Select *Start > Control Panel > Java*, then click the *Security* tab.
- 3 Modify the Security setting from *High* or *Very High* to *Medium*, then click *OK*.



- 4 Launch your web browser, then log in to Novell Remote Manager.
- 5 Generate a file inventory.
- 6 Accept the certificate warnings in order to allow the graphics to be displayed in the inventory.

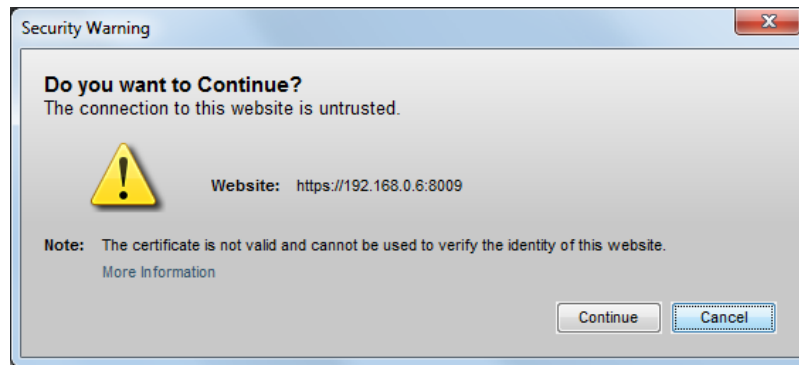
Depending on how your web browser is configured to handle unsigned certificates or self-signed certificates, you might be presented with certificate warning messages.

- ♦ **Firefox:** Each graphic is substituted with an *Activate Java Platform* notification.

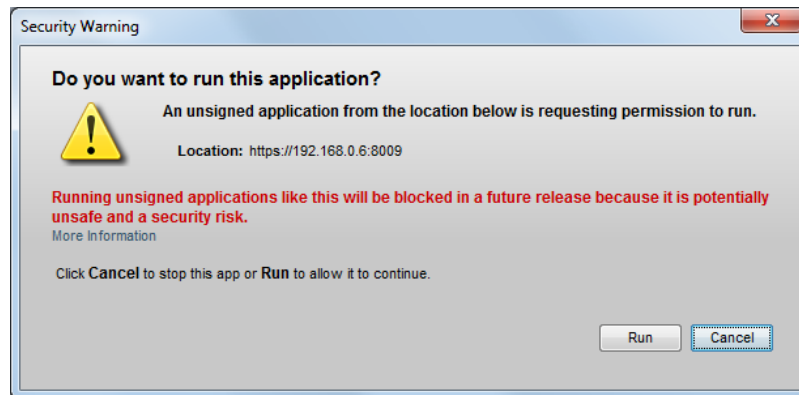
1. In the first graphic message, click the *Activate Java Platform* link to open the *Allow* pop-up menu, and then click *Allow and Remember*.



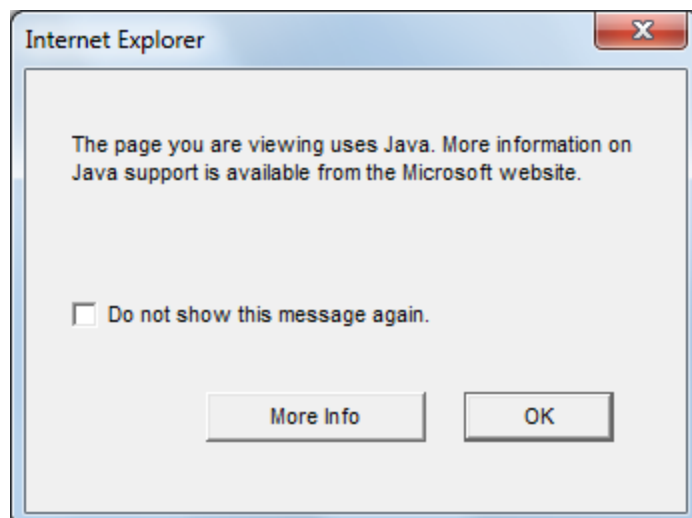
2. The first Security Warning message alerts you that the graphics application's certificate is not valid and asks if you want to continue. Click *More Information* to view information about the certificate and verify that it comes from the server, and then click *Continue*.



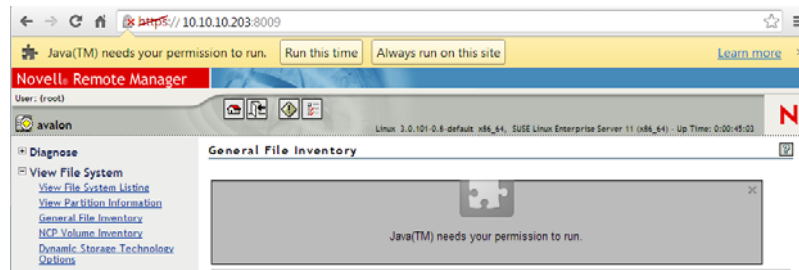
3. The second Security Warning asks your permission to run the graphics application. Click *More Information* to view information about application, and then click *Run*.



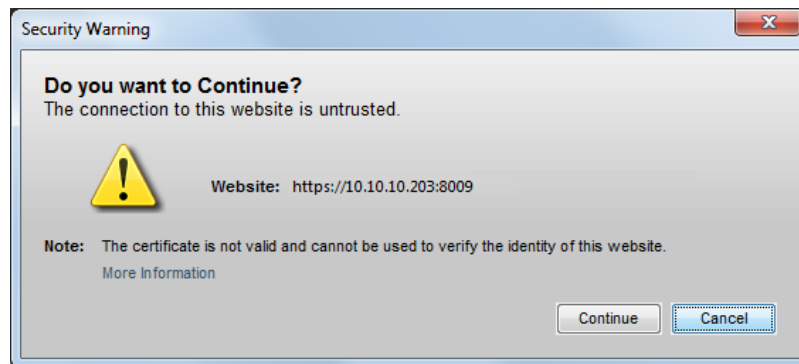
- ♦ **Internet Explorer:** When you are prompted by the certificate warning, click *More Info* to view information about the certificate and verify that it comes from the server, and then select *Do not show this message again* and click *OK*. Otherwise, a certificate warning is displayed for every graphic on the page, and you must click *OK* to dismiss each separately.



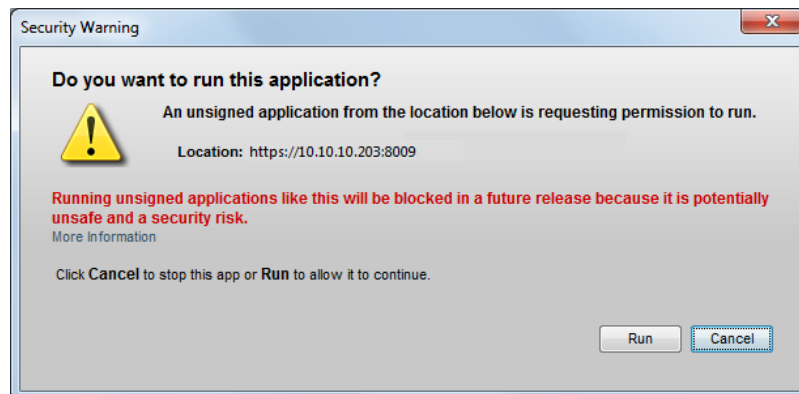
- ♦ **Chrome:** Each graphic is substituted with a *Java needs your permission to run* notification.
1. In the banner at the security warning message below the address bar, click *Always run on this site*.



2. The first Security Warning message alerts you that the graphics application's certificate is not valid and asks if you want to continue. Click *More Information* to view information about the certificate and verify that it comes from the server, and then click *Continue*.



3. The second Security Warning asks your permission to run the graphics application. Click *More Information* to view information about application, and then click *Run*.




19.5 Ganglia Statistical Graphics Are Not Displayed in the Web Browser

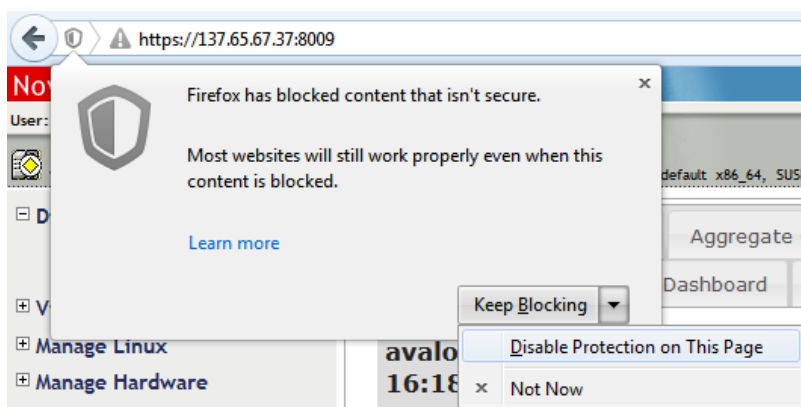
The Novell Remote Manager frame sends secure content. However, Ganglia uses scripts to graphically display statistics that send the statistical data via HTTP instead of HTTPS. Depending on how your web browser is configured to handle mixed content on a web page, the Ganglia statistics might not be displayed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

- [Section 19.5.1, “Firefox,” on page 165](#)
- [Section 19.5.2, “Internet Explorer,” on page 166](#)
- [Section 19.5.3, “Chrome,” on page 166](#)

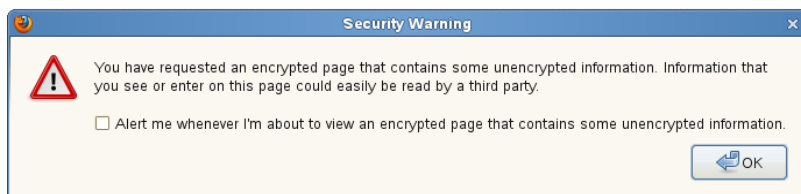
19.5.1 Firefox


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.

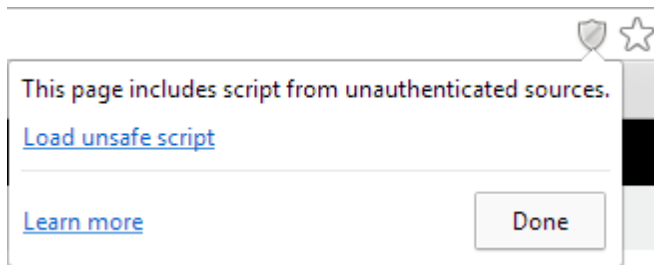
19.5.2 Internet Explorer



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.



19.5.3 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*.



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://`.

20 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 11 SP2: 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 20.1, “Security Features,” on page 167](#)
- ♦ [Section 20.2, “Security Characteristics,” on page 169](#)
- ♦ [Section 20.3, “Security Configuration,” on page 170](#)
- ♦ [Section 20.4, “Nagios Security Configuration,” on page 172](#)

20.1 Security Features

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

Table 20-1 Security Features of Novell Remote Manager on OES Linux

Feature	Yes/ No	Details
Users are authenticated	Yes	<p>Users of Novell Remote Manager must provide a user name and password credentials to log in.</p> <p>Log in as user <code>root</code>, 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.</p> <p>The <code>root</code> user is authenticated locally, not through eDirectory. This allows the <code>root</code> user to manage server resources even if the eDirectory services are not available. The <code>root</code> user has all permissions necessary to manage all functions in Novell Remote Manager.</p> <p>For more information, see “Accessing Novell Remote Manager” on page 28 and “Changing the HTTPSTKD Configuration” on page 37.</p>

Feature	Yes/ No	Details
Certificate handling by the web browser	Yes	<p>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.</p>
Limited root user privileges for the Admin user	Yes	<p>User <code>root</code> 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 <code>root</code> 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.</p> <p>The Admin user or equivalent user needs <code>root</code> 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.</p> <p><code>/etc/opt/novell/httpstkd.conf</code> <code>/etc/pam.d/httpstkd</code></p> <p>The following file names are the names that are used as the description for a specified task:</p> <p><code>/etc/cron.d/[task file name]</code></p> <p>The following files may be the actual file or a symbolic link to the YAST or eDirectory certificates:</p> <p><code>/etc/opt/novell/httpstkd/server.pem</code> <code>/etc/opt/novell/httpstkd/server.key</code></p> <p>The following files are already modifiable by the Admin user:</p> <p>The first category has names that are whatever the user names the group that they create.</p> <p><code>/opt/novell/nrm/NRMGroups/[nrm group names]</code> <code>/etc/opt/novell/nrmhconfig.conf</code> <code>/etc/opt/novell/nrmvch1thcfg.conf</code></p>
Servers, devices, and services are authenticated	Yes	<p>When gathering information with group operations, Novell Remote Manager authenticates to other servers.</p>
Access to information is controlled	Yes	<p>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.</p> <p>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.</p> <p>For more information, see “Accessing Novell Remote Manager” on page 28 and “Changing the HTTPSTKD Configuration” on page 37.</p>

Feature	Yes/ No	Details
Roles are used to control access	No	Novell Remote Manager does not have role-based management.
Logging and security auditing is done	Yes	
Data on the wire are encrypted by default	Yes	The following data are encrypted on the wire: <ul style="list-style-type: none"> ♦ Administration via browser UI ♦ When logging in the administration is switching to the HTTPS protocol.
Data is stored encrypted	No	
Passwords, keys, and any other authentication materials are stored encrypted	Yes	
Security is on by default	Yes	

20.2 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 182](#).

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 178](#).

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 20.1, “Security Features,” on page 167](#). The user Admin or equivalent user has access according to the Linux and LUM file rights to all other files.

20.3 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 20-2 Options for Changing or Limiting Access to a Server Through Novell Remote Manager

Issue/Feature	Recommendation	For More Information
SSL key cipher strength	High (112-bit or greater encryption) The default setting is ALL, which allows any encryption level.	Section A.9, "SSL Key Cipher Strength Command," on page 182
Let the root user access Novell Remote Manager with full management rights.	This is the default setting. The root user is the only user with full management rights in Novell Remote Manager.	"Accessing Novell Remote Manager" on page 28.
Let all LUM-enabled eDirectory users access file system information in Novell Remote Manager.	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.	
Deny access to all non-LUM-enabled eDirectory users.	The eDirectory users that are not LUM enabled cannot access the server through Novell Remote Manager. We recommend that the <code>root</code> 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- <code>root</code> local users.	

Issue/Feature	Recommendation	For More Information
<p>Let the <code>root</code> user access Novell Remote Manager with full management rights.</p> <p>Deny access to all LUM-enabled eDirectory users, including the Admin user and Admin-equivalent users.</p> <p>Deny access to all non-LUM-enabled eDirectory users.</p>	<p>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.</p> <p>Set the <code>nolum</code> option in the <code>/etc/opt/novell/httpstkd.conf</code> file and edit the <code>/etc/pam.d/httpstkd</code> file.</p> <p>Remove these lines:</p> <pre>auth sufficient pam_nam.so account sufficient pam_nam.so password sufficient pam_nam.so session optional pam_nam.so</pre> <p>When the <code>nolum</code> 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 <code>root</code> user has full management access to Novell Remote Manager.</p>	<ul style="list-style-type: none"> ♦ “Changing the HTTPSTKD Configuration” on page 37. ♦ “Accessing and Editing the HTTPSTKD Configuration File” on page 39.
<p>Let the <code>root</code> user access Novell Remote Manager with full management rights.</p> <p>Restrict access for all LUM-enabled eDirectory users, except the Admin user and users with rights equivalent to Admin.</p> <p>Deny access to all non-LUM-enabled eDirectory users.</p>	<p>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.</p> <p>Set the <code>supervisoronly</code> option in the <code>/etc/opt/novell/httpstkd.conf</code> file.</p> <p>When the <code>supervisoronly</code> option is set, the Admin user and Admin-equivalent users are the only LUM-enabled eDirectory users that can log in to Novell Remote Manager. They can view the file systems that they have the eDirectory rights and file system rights to see. By default, non-LUM-enabled eDirectory users continue to be denied access. Only the <code>root</code> user has full management access to Novell Remote Manager.</p>	<ul style="list-style-type: none"> ♦ “Changing the HTTPSTKD Configuration” on page 37. ♦ “Accessing and Editing the HTTPSTKD Configuration File” on page 39.
<p>Restrict access to specific workstations or a range of IP address</p>	<p>Set the <code>filteraddr</code> and <code>filtersubnet</code> options in the <code>/etc/opt/novell/httpstkd.conf</code> file.</p>	<ul style="list-style-type: none"> ♦ “Changing the HTTPSTKD Configuration” on page 37. ♦ “Accessing and Editing the HTTPSTKD Configuration File” on page 39.
<p>Remove access to the utility for all users</p>	<p>Stop the HTTPSTKD daemon.</p>	<p>“Starting or Stopping HTTPSTKD” on page 30.</p>

20.4 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 53.


A HTTPSTKD Configuration File Options

To control the behavior of Novell Remote Manager on Linux, you can specify the options listed in the HTTPSTKD configuration file in `/etc/opt/novell/httpstk.conf`. This information is in the default configuration file when installing a new server. If you modify the settings, you can view the default file settings in the `/etc/opt/novell/httpstk.conf.org` file.

If you are upgrading your server, you might need to update or add the information and settings noted if you want the applicable functionality.

To edit the `/etc/opt/novell/httpstk.conf` file in Novell Remote Manager:

- 1 Log in to Novell Remote Manager as the `root` user of the target server.
- 2 Click the  *Configure* icon in the header frame.
- 3 On the Novell Remote Manager Configuration Options page, click *HTTP Interface Management > Edit httpstk.conf file*.
- 4 Modify the settings.
- 5 To keep the changes, click *Save Changes*.

The main content frame opens to the *Directory Listing* for the `/etc/opt/novell` folder. You can verify the date and time on the file.
- 6 Restart the `httpstk` daemon to apply the changes.
 - 6a Click the  *Configure* icon to return to the Configuration Options page.
 - 6b Under *Daemon Restart*, click *Restart httpstk*.

The following options are available for controlling the behavior of Novell Remote Manager on Linux:

- ♦ [Section A.1, “Address and Port Commands,” on page 174](#)
- ♦ [Section A.2, “Disable Auto LUM Command,” on page 175](#)
- ♦ [Section A.3, “Email Notification Commands \(OES 11 SP1 and Earlier\),” on page 176](#)
- ♦ [Section A.4, “Filtering Commands,” on page 177](#)
- ♦ [Section A.5, “HttpOnly Command,” on page 178](#)
- ♦ [Section A.6, “InventoryResolveNonLumOwnerName Command,” on page 179](#)
- ♦ [Section A.7, “Language Commands,” on page 179](#)
- ♦ [Section A.8, “Load Command,” on page 181](#)
- ♦ [Section A.9, “SSL Key Cipher Strength Command,” on page 182](#)
- ♦ [Section A.10, “Supervisor Only Command,” on page 182](#)

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
```

Option	Use
IP_address	One of the following: <ul style="list-style-type: none">♦ 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: <ul style="list-style-type: none">♦ 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/ certfile_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 `no lum` option does not prevent the local-only users from logging in to Novell Remote Manager.

Use the `no lum` 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

`no lum`

Option	Use
no setting	This is the default setting.
	To perform all management functions, users must be logged in as user <code>root</code> .
	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.
	To view local file system information only, non- <code>root</code> local users can log in with their locally created user names and passwords. We recommend against creating non- <code>root</code> local users.
	When the <code>no lum</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.

Option	Use
nolum	<p>To perform all management functions, users must be logged in as user <code>root</code>.</p> <p>LUM-enabled eDirectory users are denied access. Non-LUM-enabled eDirectory users are denied access.</p> <p>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.</p> <p>IMPORTANT: Setting this option does not disable LUM if it is already part of HTTPSTKD configuration.</p> <p>You can remove the auto LUM functionality by manually by editing <code>/etc/pam.d/httpstkd</code> and removing these lines:</p> <pre>auth sufficient /lib/security/pam_nam.so account sufficient /lib/security/pam_nam.so password sufficient /lib/security/pam_nam.so session optional /lib/security/pam_nam.so</pre>

Example

nolum

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.

IMPORTANT: The Novell Remote Manager email notification system is not available beginning in OES 11 SP2.

For OES 11 SP2 and 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, 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 53](#) [Section 8.9, “Modifying the Nagios Notification Methods for Contacts,” on page 64](#).

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
```

Command	Use
no setting	Email notification is not configured. This is the default setting.
mailserver	Sends email notification to the specified mail server. You can specify up to two mail servers.
mailto	Sends email notification to the specified user. You can specify up to eight users.

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
```

Command	Use
not specified	Allows access from any address. This is the default setting.
filteraddr	Allows access from specific addresses only.
filtersubnet	Allows access from any address on the specified network or subnet.

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:

```
filteraddr 192.56.56.0 255.255.252.0
```

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>
```

Option	Use
true	Include HttpOnly as an attribute in the response header. This is the default setting.
false	Do not include HttpOnly in the response header.

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
- 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>
```

Option	Use
false	<p>The inventory does not resolve the user IDs of non-LUM-enabled file owners. The owner is reported as the Nobody user.</p> <p>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.</p>
true	<p>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.</p>

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
```

Command	Use
lang	<p>Use the following settings:</p> <ul style="list-style-type: none"> ♦ English: en en_US.UTF8 ♦ US English: en-us en_US.UTF8 ♦ Chinese Simplified: zh-cn zh_CN.UTF8 ♦ Chinese Traditional: zh-tw zh_TW.UTF8 ♦ Czech: cs cs_CZ.UTF8 ♦ French: fr fr_FR.UTF ♦ German: de de_DE.UTF8 ♦ Hungarian: hu hu_HU.UTF8 ♦ Italian: it it_IT.UTF8 ♦ Japanese: ja ja_JP.UTF8 ♦ Polish: pl pl_PL.UTF8 ♦ Portuguese-Brazil: pt pt_BR.UTF8 ♦ Russian: ru ru_RU.UTF8 ♦ Spanish: es es_ES.UTF8 ♦ Slovak: sk sk_SK.UTF8 <p>These are the default settings for this release.</p> <p>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.</p>

Example

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

```
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

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

Option	Use
<i>plug-in_file_path</i>	<code>/opt/novell/lib/</code> is the default path for Novell Remote Manager plug-in files.
<i>plug-in_file_name</i>	<code>libnrm.so</code> is a default plug-in for Novell Remote Manager.

Examples

```
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
```

Option	Use
all	Allows any negotiated encryption level. This is the default setting.
low	Allows less than 56-bit encryption.
medium	Allows 56-bit up to 112-bit encryption.
high	Allows 112-bit or greater encryption

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
```

Option	Use
no setting	<p>This is the default setting.</p> <p>Local users and all LUM-enabled eDirectory users can log in to Novell Remote Manager.</p> <p>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.</p>
supervisoronly	Lets only user <code>root</code> 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.

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.

B Novell Remote Manager Packages

[Table B-1](#) lists the packages that are installed when the Novell Remote Manager pattern is installed on an Novell Open Enterprise Server (OES) 11 SP2 server.

Table B-1 *Packages Contained in the Novell Remote Manager Pattern*

Package (RPM)	Description
novell-lum-providers	A set of CIM providers to facilitate the management of Linux User Management, which is a plug-in to PAM.
novell-nrm	Novell Remote Manager, web-based Linux machine management, and control interface. It contains all the binaries and necessary components for Novell Remote Manager.

[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*

RPM	Description
novell-ncpserv-nrm	NRM plug-in for the Novell NCP Server and Dynamic Storage Technology
novell-cifs-nrm	NRM plug-in for Novell CIFS Services
novell-afp-nrm	NRM plug-in for Novell AFP Services

[Table B-3](#) lists the software that Novell Remote Manager depends on to report server and services health information in OES 11 SP2 and later:

Table B-3 *Open Source Packages Used for Server and Services Health Monitoring in OES 11 SP2 and Later*

RPM	Description
novell-ganglia-monitor-core-gmetad	Ganglia Meta daemon that gathers the health statistics about the server
novell-ganglia-monitor-core-gmond	Ganglia Monitor daemon that provides the Ganglia monitoring service
novell-ganglia-web	Ganglia Distributed Monitoring System that provides historical graphs of the collected system metrics
nagios	Core programs for the Nagios Network Monitor
nagios-plugins	Nagios Plug-Ins that perform the service checks and return the status to Nagios
nagios-www	The HTML and CGI files for the Nagios web interface

[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*

RPM	Description
sblim-sfcb	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)
novell-hms-providers	A set of CIM providers that facilitate the gathering of data for Health Management Services (HMS)

C Documentation Updates

This section contains information about content changes that have been made in the *Novell Remote Manager Administration Guide* since the initial release of Novell Remote Manager for Novell Open Enterprise Server (OES) 11.

This document was updated on the following dates:


- ♦ [Section C.1, “January 2014 \(OES 11 SP2\),” on page 187](#)
- ♦ [Section C.2, “August 2012 \(OES 11 SP1\),” on page 192](#)

C.1 January 2014 (OES 11 SP2)

Updates were made to the following sections. The changes are explained below.

- ♦ [Section C.1.1, “Accessing Novell Remote Manager for Linux,” on page 188](#)
- ♦ [Section C.1.2, “Diagnosing Problems Using Ganglia and Nagios \(OES 11 SP2\),” on page 189](#)
- ♦ [Section C.1.3, “Diagnosing Problems Using Health Monitor \(OES 11 SP1\),” on page 189](#)
- ♦ [Section C.1.4, “HTTPSTKD Configuration File Options,” on page 189](#)
- ♦ [Section C.1.5, “Managing AFP Services,” on page 189](#)
- ♦ [Section C.1.6, “Managing CIFS Services,” on page 190](#)
- ♦ [Section C.1.7, “Managing Dynamic Storage Technology Options,” on page 190](#)
- ♦ [Section C.1.8, “Managing NCP Services,” on page 190](#)
- ♦ [Section C.1.9, “Novell Remote Manager Packages,” on page 190](#)
- ♦ [Section C.1.10, “Overview of Novell Remote Manager for Linux,” on page 190](#)
- ♦ [Section C.1.11, “Security Considerations,” on page 191](#)
- ♦ [Section C.1.12, “Troubleshooting Novell Remote Manager,” on page 191](#)
- ♦ [Section C.1.13, “Using Group Operations,” on page 191](#)
- ♦ [Section C.1.14, “Viewing File Systems,” on page 191](#)
- ♦ [Section C.1.15, “What’s New or Changed in Novell Remote Manager,” on page 192](#)

C.1.1 Accessing Novell Remote Manager for Linux

Location	Change
Section 6.1, "System Requirements," on page 27	<p>Updated web browser versions to latest versions.</p> <p>Support was added for the following web browsers:</p> <ul style="list-style-type: none">♦ Internet Explorer 10 in the desktop user interface view on Windows 7 clients and Windows 8 clients♦ Safari 6.0 on Mac OS X Mountain Lion (version 10.8) clients <p>For certificate handling, we recommend you enable your web browser for SSL 3.0 or the latest TLS if it is available.</p>
Figure 6-1, "Layout of Novell Remote Manager for OES 11 SP2," on page 31	<p>This layout is new for OES 11 SP2.</p> <p>For OES 11 SP2, 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.</p>
Section 6.2, "Accessing Novell Remote Manager," on page 28	<p>This section was reorganized for clarity.</p>
Step 3 in Section 6.2, "Accessing Novell Remote Manager," on page 28	<p>TLS 1.0 or later is also supported for SSL.</p>
Section 6.4.1, "Header Frame," on page 33	<p>Clicking the <i>Health Monitor</i> icon takes you to the Nagios Service Detail page.</p> <p>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.</p>
Section 6.4.2, "Overall Health Indicator," on page 33	<p>For OES 11 SP2, the overall health status is determined from the services you configure to be monitored and displayed on the Nagios Service Detail page.</p> <p>Clicking the <i>Server Health</i> icon takes you to the Nagios Service Detail page.</p>
Section 6.4.3, "Navigation Frame," on page 34	<p>Added links to information about the standard NRM navigation roles.</p>
Section 6.4.4, "Program Plug-Ins in the Navigation Frame," on page 35	<p>This section is new.</p> <p>The Novell CIFS plug-in allows you to manage CIFS connections on the server.</p> <p>The Novell AFP plug-in allows you to manage AFP connections on the server.</p>

C.1.2 Diagnosing Problems Using Ganglia and Nagios (OES 11 SP2)

[Chapter 8, “Diagnosing Problems Using Ganglia and Nagios \(OES 11 SP2\),” on page 45](#) is new. Beginning in OES 11 SP2, Ganglia and Nagios open source software are used to monitor server and service health.

C.1.3 Diagnosing Problems Using Health Monitor (OES 11 SP1)

Location	Change
Table 9-2, “Operating System Health Information,” on page 72	<p>For current memory, the value is the total amount of free memory that was available when the server was recently polled.</p> <p>For peak memory, the peak value is the least amount of memory that has been available while Novell Remote Manager has been running. It reports the amount of free memory available when the server's memory usage peaked during the observed interval.</p> <p>For maximum memory, the value is the total amount of memory in the system.</p>
Section 9.2, “Viewing the PIDs or Monitoring the Health of Processes,” on page 74	This section is new.
Section 9.3, “Monitoring or Killing an Individual Process,” on page 75	This section is new.

C.1.4 HTTPSTKD Configuration File Options

Location	Change
Section A.3, “Email Notification Commands (OES 11 SP1 and Earlier),” on page 176	The email notification commands <code>mailserver</code> and <code>mailto</code> in the HTTPSTKD configuration file (<code>/etc/opt/novell/httpstkd.conf</code>) are obsoleted by the notification system for Nagios. The commands are not available in the HTTPSTKD configuration file beginning in OES 11 SP2.
Section A.5, “HttpOnly Command,” on page 178	<p>The configuration file name is <code>/etc/opt/novell/httpstkd.conf</code>.</p> <p>The command name <code>HttpOnly</code> is case sensitive.</p>

C.1.5 Managing AFP Services

[Chapter 17, “Managing AFP Services,” on page 151](#) is new.

C.1.6 Managing CIFS Services

[Chapter 16, “Managing CIFS Services,” on page 147](#) is new.

C.1.7 Managing Dynamic Storage Technology Options

[Chapter 15, “Managing Dynamic Storage Technology Options,” on page 143](#) is new.

C.1.8 Managing NCP Services

[Chapter 14, “Managing NCP Services,” on page 117](#) is new. The NCP-related content was moved here from [Chapter 10, “Viewing File Systems,” on page 77](#).

Location	Change
Section 14.3.4, “Emailing a Saved NCP Inventory Report (OES 11 SP1),” on page 137	The Novell Remote Manager email notification system is not supported on OES 11 SP2. The send email option on the NCP Inventory Reports page is supported only on OES 11 SP1 and earlier.
Section 14.6.3, “Emailing a Saved NCP Trustee Report (OES 11 SP1),” on page 141	The Novell Remote Manager email notification system is not supported on OES 11 SP2. The send email option on the NCP Trustee Reports page is supported only on OES 11 SP1 and earlier.

C.1.9 Novell Remote Manager Packages

Location	Change
Table B-2, “Packages for Program Plug-Ins to Novell Remote Manager,” on page 185	This table describes the NRM plug-in packages.
Table B-3, “Open Source Packages Used for Server and Services Health Monitoring in OES 11 SP2 and Later,” on page 186	This table describes the open-source health monitoring software used by Novell Remote Manager to report server and services health information.
Table B-4, “Key Dependencies of the Novell Remote Manager Pattern in OES 11 SP1 and Earlier,” on page 186	This table describes the software used by Novell Remote Manager to report system health information.

C.1.10 Overview of Novell Remote Manager for Linux

Location	Change
Table 1-2, “Information about Plug-Ins to Novell Remote Manager,” on page 13	This table links to quick references about the plug-in in this guide and to the books for the related OES Services.

C.1.11 Security Considerations

Location	Change
"Certificate handling by the web browser" on page 168	Certificate handling requires SSL 2.0 or later, or TLS 1.0 or later, to be enabled in your web browser. We recommend the higher security options of SSL 3.0, or the latest TLS if it is available.

C.1.12 Troubleshooting Novell Remote Manager

Location	Change
Section 19.2, "Error while loading shared libraries: libldapx.so.0," on page 159	This section is new.

C.1.13 Using Group Operations

Location	Change
Section 13.1, "Building and Configuring a Monitoring Group," on page 104	The Web Page monitoring option shows the response when trying to determine if the communication is working to a server that hosts a website.
Section 14.6.3, "Emailing a Saved NCP Trustee Report (OES 11 SP1)," on page 141	The Novell Remote Manager email notification system is not supported on OES 11 SP2. The Email Options on the Group Operations Configuration page are supported only on OES 11 SP1 and earlier.

C.1.14 Viewing File Systems

Location	Change
Section 14.2.5, "Salvaging and Purging Deleted Files on an NSS Volume," on page 132	<p>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.</p> <p>You can also select a deleted directory and use the Purge option to purge the deleted directory and all of the deleted subdirectories and files that it contains.</p>

Location	Change
"Performing Actions on Files from Custom Reports" on page 139	Actions on files in the inventory are performed in the selected volume. The target path must be to a location on the same volume.

C.1.15 What's New or Changed in Novell Remote Manager

Location	Change
Section 2.1, "What's New (OES 11 SP2)," on page 15	This section is new.

C.2 August 2012 (OES 11 SP1)

Updates were made to the following sections. The changes are explained below.

- [Section C.2.1, "Managing a Virtualized Linux Server with Novell Remote Manager," on page 192](#)
- [Section C.2.2, "Viewing File Systems," on page 192](#)
- [Section C.2.3, "What's New or Changed in Novell Remote Manager," on page 192](#)

C.2.1 Managing a Virtualized Linux Server with Novell Remote Manager

Location	Change
Chapter 4, "Managing a Virtualized Linux Server with Novell Remote Manager," on page 23	KVM is supported in OES 11 SP1 and later.

C.2.2 Viewing File Systems

Location	Change
Section 14.3, "Generating Inventories for Directories or NCP Volumes," on page 133	File ownership information can now be retrieved for files on NSS volumes without needing to enable users with Linux User Management.
Section 14.6, "Generating and Viewing NCP Trustee Reports for NSS Volumes," on page 140	This section is new.

C.2.3 What's New or Changed in Novell Remote Manager

Location	Change
Section 2.2, "What's New (OES 11 SP1)," on page 17	This section is new.