Veritas™ Operations Manager 4.0 Administrator's Guide
Veritas™ Operations Manager Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 4.0
Documentation version: 4.0.1

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec logo, Veritas, and Veritas Storage Foundation are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement. 
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

**Licensing and registration**

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:


**Customer service**

Customer service information is available at the following URL:


Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

- Asia-Pacific and Japan: customercare_apac@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec’s enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management
Chapter 1 Basic Veritas Operations Manager tasks .......................... 19
About the communication between the managed hosts and Management Server ...................................................................... 19
Setting up Internet Explorer 7.0 and Firefox 3.0 for Veritas Operations Manager ........................................................................ 21
Connecting to Veritas Operations Manager .............................................................................................................................. 22
Verifying the version of Veritas Operations Manager Management Server in the console .............................................................. 23
Verifying the version of a Veritas Operations Manager managed host in the console ........................................................................ 24
Administering a UNIX or a Windows managed host .......................... 24
Stopping and starting the Web application ...................................... 25

Chapter 2 Configuring Management Server settings ......................... 27
About the methods to enhance the availability of Management Server .................................................................................................... 27
Viewing the Management Server settings ........................................ 28
Configuring SMTP settings for email notifications .............................. 29
Enabling the analytic gathering on Management Server ................. 30
Setting the period for retaining the alert and the task logs in the Veritas Operations Manager database ..................................................... 31
About configuring Web server settings in Veritas Operations Manager .................................................................................................... 32
Configuring the Web server settings in Veritas Operations Manager .................................................................................................... 32
Viewing the details of active users logged in to Management Server .................................................................................................... 33

Chapter 3 Managing Veritas Operations Manager alerts ................. 35
About faults and risks ...................................................................... 36
Viewing faults and risks .................................................................. 37
About analyzing faults ...................................................................... 37
Analyzing faults in Veritas Operations Manager .......................... 38
Suppressing faults ........................................................................ 40
  Suppress the Faults options ..................................................... 40
Viewing the faults definitions ..................................................... 41
Suppressing the fault definitions .................................................. 42
  Suppress the fault definition options ......................................... 43
Activating suppressed fault definitions ......................................... 43
  Activate the suppressed fault definition options ....................... 44
Activating suppressed faults ....................................................... 44
About alerts ................................................................................ 44
About alert rules .......................................................................... 45
Viewing alert rules ....................................................................... 46
Creating alert rules ..................................................................... 47
  Create Rule - Alert Conditions options ..................................... 48
  Create Rule - Select Alerts options .......................................... 49
  Create Rule - Trigger Alert Source options ................................. 50
  Create Rule - Setup notifications options .................................. 50
  Create Rule - Description ...................................................... 53
Viewing the overview of a rule ..................................................... 54
Modifying alert rules ................................................................... 54
  Edit Rule - Alert Conditions options ....................................... 56
  Edit Rule - Select Alerts options .............................................. 57
  Edit Rule - Trigger Alert Source options .................................... 57
  Edit Rule - Setup notifications options ..................................... 58
  Edit Rule - Name options ....................................................... 60
Copying alert rules ....................................................................... 61
  Copy Rule options .................................................................. 62
Enabling alert rules ...................................................................... 62
Disabling alert rules ..................................................................... 63
Deleting alert rules ...................................................................... 64
  Delete an Existing Rule options ............................................... 64
Viewing alerts ............................................................................. 64
  Alert Log Details options ....................................................... 66
About tasks ................................................................................ 67
Viewing tasks ............................................................................. 67
About messages posted on Activity Board ................................. 68
Viewing the messages posted on Activity Board ........................... 68
Deleting a message that is posted on Activity Board .................... 68
Chapter 4  Deploying Veritas Operations Manager solutions ................................................................. 71

About Veritas Operations Manager solutions ................................................................. 72
About deploying Veritas Operations Manager solutions ................................................... 72
  About deploying add-ons ............................................................................................... 73
  About deploying packages or patches ............................................................................. 75
  About deploying hotfixes ............................................................................................... 76
Viewing Veritas Operations Manager solutions in the repository .......................................................... 76
Uploading a solution to repository ..................................................................................... 77
Installing Veritas Operations Manager solution .................................................................... 78
  Install solution options ................................................................................................. 79
Upgrading managed hosts using Veritas Operations Manager console .............................................................. 80
Uninstalling a solution ......................................................................................................... 81
Removing a Veritas Operations Manager solution from repository .................................................. 82
Viewing the solution deployment summary and the hosts to install solution .................................................. 82
Installing solutions on specific managed hosts ........................................................................ 84
Uninstalling solutions from specific managed hosts ........................................................................ 84
Enabling the solution on specific managed hosts ...................................................................... 84
  Enable solutions on specific managed hosts options ......................................................... 85
Disabling the solution on specific managed host ...................................................................... 85
  Disable solutions on specific managed hosts options ......................................................... 86
Viewing the deployment requests for a solution ........................................................................ 86
  Viewing deployment request details for a solution ............................................................. 87
Canceling the deployment request for a solution ......................................................................... 87
  Downloading the deployment log for a solution's deployment request ................................ 88

Chapter 5  Managing databases in Veritas Operations Manager ................................................................. 91

Performing the database discovery for secure databases ........................................................... 91
  Select database instances options ................................................................................... 93
  Provide credentials options .............................................................................................. 93
  Database Instance Credentials Summary ........................................................................... 93

Chapter 6  Managing clusters in Veritas Operations Manager ................................................................. 95

Viewing the fire drill schedules ............................................................................................... 95
  Modifying a fire drill schedule .......................................................................................... 96
Chapter 7  Managing hosts in Veritas Operations Manager .......... 99
About managing the hosts from Management Server .............. 100
Viewing the details of the managed hosts associated with Management Server .......................................................... 101
Configuring the managed hosts to Management Server using the Web Console .......................................................... 102
Configure host options .......................................................... 103
Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script ............................................. 104
Refreshing the details of the managed host .............................. 107
Removing the managed hosts from Management Server ............ 107
About monitoring usage and configuring the automatic growth for file systems .......................................................... 108
Setting the threshold for monitoring file system usage ............... 109
Monitor Capacity panel options ............................................. 110
Monitor Capacity Summary panel options ............................. 111
Configuring the automatic growth of the file systems ............... 112
About using Veritas Operations Manager to manage the hosts with Symantec ApplicationHA ............................................. 113
Enabling application heartbeat for a service group ..................... 114
Disabling application heartbeat for a service group ................... 115

Chapter 8  Discovering the server virtualization environment using Veritas Operations Manager .......... 117
About the virtualization technologies supported by Veritas Operations Manager ......................................................... 118
About Control Hosts in Veritas Operations Manager .................. 119
About discovering the VMware Infrastructure using Veritas Operations Manager ......................................................... 121
Requirements for discovering VirtualCenter and ESX servers using Veritas Operations Manager ...................................... 123
How Veritas Operations Manager discovers VirtualCenter and ESX servers .......................................................... 124
Information that Veritas Operations Manager discovers on the VMware Infrastructure components .............................. 125
About the datastores in Veritas Operations Manager .................. 125
Limitations of the discovery of VirtualCenter and ESX servers using Veritas Operations Manager ...................................... 126
Viewing the Virtualization Management view ................................ 126
Configuring the VMware discovery in Veritas Operations Manager .......................................................... 127
Virtualization Configuration panel options .............................. 128
Virtualization Configuration progress details panel .................... 130
Editing a VMware discovery configuration in Veritas Operations
Manager ................................................................. 130
Virtualization Configuration panel options (Edit) .................... 131
Virtualization Configuration progress details panel (Edit) ............ 132
Refreshing a VMware discovery configuration in Veritas Operations
Manager ................................................................. 132
Removing a VMware discovery configuration in Veritas Operations
Manager ................................................................. 133
About discovering Solaris zones in Veritas Operations Manager .......... 134
Requirements for discovering Solaris zones in Veritas Operations
Manager ................................................................. 135
How Veritas Operations Manager discovers Solaris zones .......... 136
Information that Veritas Operations Manager discovers on
Solaris zones ................................................................. 137
Limitations of the discovery of Solaris zones in Veritas
Operations Manager ....................................................... 138
About discovering Logical domains in Veritas Operations
Manager ................................................................. 139
Requirements for discovering Solaris Logical domains using
Veritas Operations Manager ............................................. 140
How Veritas Operations Manager discovers Solaris Logical
domains ........................................................................ 141
Information on Logical domains that Veritas Operations Manager
discovers ................................................................. 142
Limitations of the discovery of Logical domains in Veritas
Operations Manager ....................................................... 142
About the reports related to virtualization in Veritas Operations
Manager ................................................................. 143
Viewing the summary of virtualization in Veritas Operations
Manager ................................................................. 143
Viewing virtualization servers in Veritas Operations Manager ............ 144
Viewing the virtual machines in Veritas Operations Manager ............. 146

Chapter 9 Managing storage enclosures in Veritas Operations
Manager ................................................................. 149
Setting display name for a storage enclosure ............................ 149
Set displayable name for enclosure options ............................ 150
Set displayable name for array port options ............................ 150
Setting display name for an array port ................................... 151
### Chapter 10: Downloading Storage Foundation and Storage Foundation and High Availability patches using Symantec Operations Readiness Tools

- Viewing the patches available to a host ........................................... 153
- Viewing the details of a patch in the SORT Web site ......................... 154
- Setting up proxy server details to download patch information .......... 155
  - Proxy server and download schedule settings options ..................... 156
- Downloading patch information in offline mode ............................... 156

### Chapter 11: Monitoring performance in Veritas Operations Manager

- About Veritas Operations Manager performance graphs ................. 159
- Viewing the performance graphs for a volume ................................. 161
- Viewing the performance graphs for a host ..................................... 162
- Viewing the performance graphs for a disk ..................................... 163
- Viewing the performance graphs for an initiator .............................. 164
- Viewing the performance graphs for a file system ......................... 165
- Comparing the performance of volumes ........................................ 167
- Comparing the performance of disks .............................................. 168
- Comparing the performance of initiators ........................................ 169
- Comparing the performance of hosts ............................................. 170
- Comparing the performance of file systems .................................... 171

### Chapter 12: Managing Security groups in Veritas Operations Manager

- About the security model for Veritas Operations Manager ................. 173
- About predefined roles in Veritas Operations Manager ...................... 174
- Viewing security group details in Veritas Operations Manager .......... 180
- Adding security groups to the Veritas Operations Manager domain .................................................. 182
  - New Security Group options .................................................. 183
- Modifying the security groups in the Veritas Operations Manager domain .................................................. 186
  - Edit Access Control options .................................................. 186
- Removing security groups from Veritas Operations Manager .......... 188
Add to Business Entity options ................................................ 210
Making a business entity available to the security groups in Veritas
Operations Manager ............................................................. 210
Change Permissions options ................................................... 211
Setting the extended attributes on a business entity ......................... 211
Select base object type options ................................................ 212
Select related object types options ........................................... 213

Chapter 14 Managing Authentication Brokers in Veritas
Operations Manager ............................................................. 215

About managing Authentication Brokers in the Veritas Operations
Manager domain .................................................................. 216
About managing domains associated with an Authentication Broker
in Veritas Operations Manager ............................................... 217
Viewing the details of the Authentication Brokers and the domains
associated with them ............................................................ 218
Adding secondary Authentication Brokers to the Veritas Operations
Manager domain .................................................................. 219
Add New Broker options ........................................................ 221
Refreshing the information associated with the Authentication
Brokers ............................................................................... 222
Removing the Authentication Brokers from the Veritas Operations
Manager domain .................................................................. 222
Configuring Lightweight Directory Access Protocol-based
authentication on the Management Server host ......................... 223
LDAP/AD Settings - discover attributes and configuration
information panel options ................................................ 224
LDAP/AD Settings - configure LDAP based authentication
options ......................................................................... 226
Removing Lightweight Directory Access Protocol or Active Directory
configuration from the primary Authentication Broker ............... 228
Enabling the authentication domains associated with an
Authentication Broker ........................................................... 229
Enable Domains options ........................................................ 230
Disabling the authentication domains associated with an
Authentication Broker ........................................................... 230
Disable Domains options ........................................................ 231

Chapter 15 Managing licenses in Veritas Operations
Manager .............................................................................. 233

About License Deployment Report ................................................. 234
Advantages of using License Deployment Report .............................. 236
Chapter 16  Viewing deployment information in Veritas Operations Manager ................................. 257

About License Deployment Summary view .................................................. 258
About the product inventory summary .................................................... 259
About the product-tier mapping summary .......................................... 260
About the Tier-Host Mapping summary ............................................. 261
About License Deployment detailed view ............................................. 262
About the exceptions summary .......................................................... 263
Viewing the License Deployment Summary view ................................. 263
Viewing the summary of product inventory ......................................... 267
Viewing the Product-Tier Mapping summary ...................................... 269
Viewing the Tier-Host Mapping summary ......................................... 271
Viewing a product overview ............................................................. 271
Viewing product details by host name ............................................... 272
Viewing the evidence details of a feature in Veritas Operations Manager ........................................... 274
Viewing the overview of a host .......................................................... 275
Viewing the overview of the licenses information for a host ............... 277
Chapter 17 Using Policy Check ............................................................ 289

About Policy Check ..................................................................... 290
About policy templates ............................................................... 290
About creating policy templates .................................................... 291
Creating policy templates ............................................................ 292
    Policy Template Details options ............................................ 293
    Select Signatures options ............................................... 293
    Select Scope options ....................................................... 294
    Specify Schedule options ................................................ 294
    Policy Template Summary options ..................................... 295
Modifying policy templates ........................................................ 296
Running a manual policy template scan .......................................... 297
Deleting a policy template ............................................................ 297
About policy violations ................................................................ 298
Marking policy violations to exclude from the subsequent scans ......... 298
About Installed Signatures ........................................................... 299
About the customized signature in Veritas Operations Manager for
    identifying risks ................................................................... 300
About creating a customized signature script .................................. 301
Sample customized signature script ............................................. 302
About registering the customized signature .................................... 304
About copying the customized signature script ............................ 304
About using the Distribution Manager Add-on to bundle a
    customized signature .......................................................... 305
About removing a customized signature from Veritas Operations
    Manager ............................................................................ 308
Adding signatures to a policy template .......................................... 308
Setting signature tunables ........................................................... 308
    Set Signature Tunables options ........................................ 309
Removing a signature from a policy template .................................. 309
Deleting a policy template scan ..................................................... 310
Viewing scan tunables associated with a policy scan ......................... 310
Chapter 18 Managing reports in Veritas Operations Manager

About managing reports .............................................................. 313
Running a report ................................................................. 315
   Select Scope options ......................................................... 315
Creating a report schedule ...................................................... 316
   Schedule options ............................................................. 317
   Specify Schedule Details options ....................................... 317
Editing a report schedule ......................................................... 318
Enabling a report schedule ...................................................... 319
Disabling a report schedule .................................................... 319
Removing a report schedule .................................................... 319
Archiving reports ................................................................. 320
   Archive Report Data options ............................................ 321
Sending a report through email ............................................... 321
   Email Archived Report options ....................................... 322
   Email Report Data options .............................................. 322
Deleting an archived report ..................................................... 323
Exporting report data to a file ............................................... 323

Chapter 19 Managing schedules in Veritas Operations Manager

About managing schedules in Veritas Operations Manager ........ 325
Enabling schedules ............................................................... 326
Disabling schedules ............................................................... 327
Deleting schedules ............................................................... 327

Chapter 20 Managing Dynamic Multipathing paths in Veritas Operations Manager

About using the Veritas DMP Maintenance functionality in Veritas Operations Manager ................................. 329
Disabling the DMP paths on an array ...................................... 330
   Start panel options .......................................................... 330
   Select Enclosure panel options ........................................ 333
   Specify Array Port(s) panel options .................................. 334
   Path Disable Confirmation panel options ......................... 334
   Veritas DMP Maintenance Associations Report ................ 335
   Paths Disabled panel options ......................................... 336
Disabling the DMP paths on an initiator ................................. 336
Basic Veritas Operations Manager tasks

This chapter includes the following topics:

■ About the communication between the managed hosts and Management Server
■ Setting up Internet Explorer 7.0 and Firefox 3.0 for Veritas Operations Manager
■ Connecting to Veritas Operations Manager
■ Verifying the version of Veritas Operations Manager Management Server in the console
■ Verifying the version of a Veritas Operations Manager managed host in the console
■ Administering a UNIX or a Windows managed host
■ Stopping and starting the Web application

About the communication between the managed hosts and Management Server

Veritas Operations Manager provides you a single, centralized management console for the Storage Foundation and High Availability products. You can use it to monitor, visualize, and manage storage resources and generate reports about them. Veritas Operations Manager lets administrators centrally manage diverse datacenter environments.

A typical Veritas Operations Manager deployment consists of a Management Server and the managed hosts. The managed host can run on any platform that Veritas Operations Manager supports. In a centrally managed deployment, you
must configure one host as Management Server. Management Server receives information about all the resources in its domain. When you log on to Management Server, you can gain access to the resources on different hosts within the centrally-managed deployment.

The .bin file installs the VRTSsfmcs (Management Server) and the VRTSsfmh (managed host) packages on the host that is designated as Management Server. The VRTSsfmh package contains the XPRTL component that facilitates the communication between the managed hosts and Management Server. The VRTSsfmh is installed on the managed host and the Management Server.

The XPRTL component consists of the following:

- The XPRTLD component, which is a light weight and full-featured Web server.
- The XPRTLC component, which is an HTTP client that is based on command lines. The XPRTLC component can send information to Web servers.

The XPRTLD and the XPRTLC components are integrated with Veritas Authentication Services for secure SSL communication over HTTP.

The communication between the managed host and Management Server occurs through the HTTPS protocol. The XPRTLD Web server running on both the managed host and Management Server supports the Common Gateway Interface (CGI) standards. The managed hosts use XPRTLC and invoke CGI through the XPRTLD on the Management Server to perform several actions such as the Veritas Operations Manager database update. The Management Server uses XPRTLC and invokes CGI through the XPRTLD on the managed hosts to perform various actions that include Storage Foundation and high availability operations.

The following table describes the frequency of the managed host information updates in the Management Server database. The discovery on each managed host is divided into families to focus on a particular functional area:

<table>
<thead>
<tr>
<th>Family</th>
<th>Frequency in minutes</th>
<th>Discovered information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>1440</td>
<td>The operating system, licenses, packages, and networking for the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Typically, most of the information that is related to this family do not change frequently.</td>
</tr>
<tr>
<td>Storage Foundation</td>
<td>30</td>
<td>Volume Manager, File Systems, and the related storage network.</td>
</tr>
<tr>
<td>Family</td>
<td>Frequency in minutes</td>
<td>Discovered information</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Veritas Cluster Server</td>
<td>60</td>
<td>Veritas Cluster Server and the related information</td>
</tr>
<tr>
<td>Databases</td>
<td>60</td>
<td>Oracle, DB2, MSSQL, and Sybase databases and their storage dependencies.</td>
</tr>
<tr>
<td>NR</td>
<td>5</td>
<td>Configuration status and external faults.</td>
</tr>
<tr>
<td>Native</td>
<td>360</td>
<td>Third Party Volume Management information.</td>
</tr>
</tbody>
</table>

**Note:** The discovery for the Storage Foundation and Veritas Cluster Server families are event driven. This means that the discovery is triggered when configuration changes occur in the managed hosts. As a result, this information must be updated in the Veritas Operations Manager database in the following update. If configuration changes are not detected on the managed hosts, the communication between the managed host and Management Server is restricted to the heartbeat communication that occurs every five minutes.

### Setting up Internet Explorer 7.0 and Firefox 3.0 for Veritas Operations Manager

If you use Internet Explorer 7.0 on Windows Server 2008, or Firefox 3.0, the web pages for configuring and launching Veritas Operations Manager are not displayed. You need to set up the Web browser to display the Web pages. For Internet Explorer 7.0 on Windows Server 2008, if the Web pages are not automatically displayed, add each Web site to the **Trusted Sites** list. On Firefox 3.0, if a security exception is displayed, add the exception to the Web browser to override how Firefox identifies the sites.

**To set up Internet Explorer 7.0 on Windows Server 2008 for Veritas Operations Manager**

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. Select the **Security** tab.
3. Click **Sites** to add the following Web sites:
   - **https://hostname:5634**/—URL to configure Veritas Operations Manager
   - **https://hostname:14161**/—URL to launch Veritas Operations Manager
where, hostname is the name of the Management Server host.

To set up Firefox 3 for Veritas Operations Manager

1 On the security exception page that is displayed when you attempt to open an Veritas Operations Manager Web page, click the **Or you can add an exception** link.

2 Click **Add Exception**.
   For Firefox 3.6.x, the users should first click the **I Understand the Risks** button before they click the **Add Exception** button.

3 In the **Add Security Exception** dialog, verify that the location is one of the following:
   - **https://hostname:5634/** — URL to configure Veritas Operations Manager
   - **https://hostname:14161/** — URL to launch Veritas Operations Manager
   where, hostname is the name of the Management Server host.

4 Click **Get Certificate**.

5 Select the **Permanently store this exception** check box.

6 Click **Confirm Security Exception**.
   The Web page is now displayed.

Connecting to Veritas Operations Manager

After downloading the installation files, you must install and configure Veritas Operations Manager. For more information on installation and configuration, refer to *Veritas™ Operations Manager Installation Guide 4.0*.

You can use any supported Web browser to connect to Veritas Operations Manager.
To connect to Veritas Operations Manager

1. On a client system that has a network connection to the host, open a Web browser.

   Your browser must be configured to accept cookies. If you are using pop-up blockers, either disable them or configure them to accept pop-ups from the host.

2. In the browser’s address field, type the following URL and press Enter:

   `https://hostname:14161/`

   where `hostname` is the host name, fully-qualified host name, or IP address of the Management Server.

   Example: `https://myhost.example.com:14161/`

   For Internet Explorer 7.0 on Windows Server 2008, or Firefox 3.0, if the Web page does not get displayed, you have to set up the browser.

   See “Setting up Internet Explorer 7.0 and Firefox 3.0 for Veritas Operations Manager” on page 21.

3. In the `username` and `password` fields, type credentials for a valid operating system network domain account.

   The AuthenticationService automatically recognizes users in the domain—for example, unixpwd or NT—on which the Authentication Broker host is a member.

4. Click Login.

   You can view the Veritas Operations Manager Dashboard.

---

Verifying the version of Veritas Operations Manager Management Server in the console

After you have installed or upgraded Management Server, you can verify its version in the Veritas Operations Manager console.

To verify the version of Management Server in the console

1. In the header, at the top of the Veritas Operations Manager console, click About.

   The Management Server version is displayed.

2. To close the window, click OK.

   See “Verifying the version of a Veritas Operations Manager managed host in the console” on page 24.
Verifying the version of a Veritas Operations Manager managed host in the console

After you have installed or upgraded a managed host, you can verify its version in the Veritas Operations Manager console.

To verify the version of a managed host in the console

1. In the Veritas Operations Manager console, click **Settings > Host Management**.

2. In the **Host Management** view that is displayed, verify the managed host version in the **MH Version** column.

See “Verifying the version of Veritas Operations Manager Management Server in the console” on page 23.

Administering a UNIX or a Windows managed host

You can perform the Storage Foundation tasks on a UNIX or a Windows managed host. You can perform the Storage Foundation tasks after you install Storage Foundation Administration for Unix Add-on and Storage Foundation Administration for Windows Add-on.

In Veritas Operations Manager 4.0, the prebundled Veritas Operations Manager Add-on for Storage Foundation Administration lets you do some of the important Storage Foundation tasks without using the **Administer** link on the Veritas Operations Manager console. In the Veritas Operations Manager console, you can select multiple objects to perform operations on them simultaneously in a batch.

Using the Veritas Operations Manager Add-on for Storage Foundation Administration, you can perform the Storage Foundation operations for the following storage objects:

- The volumes and the disk groups that are managed by Veritas Volume Manager.
- The disks that are controlled by Veritas Volume Manager.
- The native file systems and the Veritas File System that are mounted on the Storage Foundation volumes.

The Veritas Operations Manager Add-on for Storage Foundation Administration is enabled by default in Veritas Operations Manager.

For more information on using the Veritas Operations Manager Add-on for Storage Foundation Administration, refer to *Veritas Operations Manager Add-on for Storage Foundation Operations 4.0 User's Guide*.
You must have the administrator privileges on a UNIX or a Windows managed host to perform the Storage Foundation tasks on them.

**Note:** In Veritas Operations Manager, the managed hosts on the HP-UX 11.11 platform that contain the Storage Foundation 3.5 stack is supported in read-only mode. The **Administer** link for these managed hosts is disabled.

**To administer a UNIX or a Windows managed host**

1. In Veritas Operations Manager console, select **Manage > Hosts**.
2. In the **Hosts** view, in the table that lists the hosts, click the name of the host that you want to administer.
3. In the details view of the host, at the bottom of the the Breadcrumb bar that shows the navigation path to the current page, on the task toolbar, click **Administer**.

   If the **Administer** link has a red arrow that is displayed after it, you cannot perform the UNIX or the Windows managed host administration.

See “About Veritas Operations Manager solutions” on page 72.

---

**Stopping and starting the Web application**

You can stop and restart the Veritas Operations Manager Web UI framework.

**To stop and restart the Veritas Operations Manager Web UI framework**

1. Open an operating system console and log on as root to Management Server.
2. Depending on the platform of Management Server, use one of the following to restart the Veritas Operations Manager Web UI framework:
   - **Solaris and Red Hat Linux:** Execute the `/opt/VRTSsfmcscweb/sfmw restart` command.
   - **Windows:** Under Service Control Manager (**services.msc**), restart the **Storage Manager Service** service.
Basic Veritas Operations Manager tasks

Stopping and starting the Web application
Configuring Management Server settings

This chapter includes the following topics:

- About the methods to enhance the availability of Management Server
- Viewing the Management Server settings
- Configuring SMTP settings for email notifications
- Enabling the analytic gathering on Management Server
- Setting the period for retaining the alert and the task logs in the Veritas Operations Manager database
- About configuring Web server settings in Veritas Operations Manager
- Configuring the Web server settings in Veritas Operations Manager
- Viewing the details of active users logged in to Management Server

About the methods to enhance the availability of Management Server

In Veritas Operations Manager, you have the following three methods to enhance the availability of Management server:

- Configure more than one host as Management Servers in your datacenter: Veritas Operations Manager lets the managed hosts in your datacenter to report to more than one Management Servers. Therefore, you can configure more than one host in your datacenter as Management Servers to enhance their availability.
 ■ Configure Veritas Operations Manager in high availability environment:
Configuring Veritas Operations Manager in high availability environment (Veritas Operations Manager HA configuration) enhances the availability of Management Server. Also, this configuration improves the availability of the applications and the services that Veritas Operations Manager provides. For the Veritas Operations Manager HA configuration, you must use a two-node VCS cluster in which Storage Foundation HA 5.0 is installed.
For additional information, refer to *Veritas Operations Manager Installation Guide*.

 ■ Configure the disaster recovery feature on the Veritas Operations Manager HA configuration:
You can configure the disaster recovery feature on Veritas Operations Manager that is configured in high availability environment. This configuration enhances the failover support and the availability of Management server in your globally distributed datacenter. You must replicate the Veritas Operations Manager database and the domain-wide information that is stored in the shared storage to the second site as part of configuring the disaster recovery feature.
For additional information, refer to *Veritas Operations Manager Installation Guide*.

---

**Viewing the Management Server settings**

The **Management Server Settings** view lets you do the following:

 ■ Configure the SMTP settings for Management Server.
 ■ Enable the analytics gathering on Management Server.
 ■ Set proxy server details to download patch information.
 ■ Download patch information in offline model.
 ■ Set the database retention policy.
 ■ Set log levels and webserver session timeout.
 ■ View the details of the active users who have logged in to Management Server.

**To view the Management Server settings**

◆ In Veritas Operations Manager console, select **Settings > Management Server** to view the Management Server settings in the **Management Server Settings** view.

See “**Configuring SMTP settings for email notifications**” on page 29.
See “**Enabling the analytic gathering on Management Server**” on page 30.
Configuring SMTP settings for email notifications

In the Settings > Management Server view, you can configure the SMTP settings for Management Server. Under SMTP Settings, you must enter the following details:

- **SMTP Server**: Enter the SMTP mail server host name. Valid formats include: Fully Qualified Domain Name (FQDN), IP address, or, if the network handles DNS resolution for host names, a shortened host name.
  
  Examples:
  
  Host123, Host123.example.com, xxx.yyy.zzz.aaa

- **SMTP Port**: Enter the SMTP mail server port number.

- **Sender Account**: Enter a valid email address for the sender. This email address appears as the sender of all the emails that a rule sends out.
  
  Example: user@example.com

**Note**: Before you specify the email notifications for alert rules or policy check scan completion, or send a report by email, you must configure the SMTP details for Management Server.

Also, you can send a test email to the recipient’s account to verify the SMTP settings that you have configured. To send the test email, you must enter the following details:

- **Recipient Account**: Enter a valid email address of the recipient.
Enter the test email message that you want to send to the recipient.

To configure SMTP settings for email notifications
1. In the Veritas Operations Manager console, select Settings > Management Server.
2. Under SMTP Settings, enter the SMTP details and click Save Settings.

To verify the SMTP settings
1. Under SMTP Settings, click Test SMTP to display the fields where you must enter the details for verifying the SMTP settings.
2. Enter the valid email address of the recipient and the test email message. Click Send Test Mail.

See “Viewing the Management Server settings” on page 28.

Enabling the analytic gathering on Management Server

Veritas Operations Manager uses web beacons (also known as single pixel or clear GIFS) to provide statistical information such as the frequency of use of particular features or views of the Veritas Operations Manager user interface in your organization to help analyze product usage. The information does not identify the users. Symantec analyzes this data to understand the information that is of most interest to the customers and the features that the customers use most.

In the Management Server Settings view, you can enable the analytics gathering on Management Server.

If the Enable Analytics Gathering option is enabled while you configure the Management Server, the Enable Analytics Gathering check box appears selected. You can clear the Enable Analytics Gathering option selection to disable the analytics gathering on Management Server.

To enable analytic gathering on Management Server
1. In Veritas Operations Manager console, select Settings > Management Server.
2. In the Management Server Settings view, under Analytics Gathering Settings, select the Enable Analytics Gathering check box and click Save Settings.

See “Viewing the Management Server settings” on page 28.
Setting the period for retaining the alert and the task logs in the Veritas Operations Manager database

In the Management Server Settings view, you can set the period for retaining the alert and the task logs. After this period, the alert and the task logs are removed from the Veritas Operations Manager database.

You must enter the following details for setting the period for retaining the alert and the task logs:

Alert Log

Select the period for which you want to retain the alert logs in the Veritas Operations Manager database.

You can select one of the following options:

- 7 days
- 15 days
- 21 days
- 30 days.

Task Log

Select the period for which you want to retain the task logs in the Veritas Operations Manager database.

You can select one of the following options:

- 7 days
- 15 days
- 21 days
- 30 days.

To set the period for retaining the alert and the task logs in the Veritas Operations Manager database

1. In the Veritas Operations Manager console, select Settings > Management Server.
2. Under Database Retention Policy Settings, set the period for retaining the alert and the task logs and click Save Settings.

See “Viewing the Management Server settings” on page 28.
About configuring Web server settings in Veritas Operations Manager

In the Management Server Setting page, Veritas Operations Manager helps you configure the following:

- Log level for the log files in the Web server.
- User session timeout period for the Web server.

You can set the levels of the Web server log as Severe, Warning, Info, or Debug. By default, the log level is set as Info. Also, Veritas Operations Manager lets you specify whether you need a cumulative log record for all the Web server sessions that you have used.

Veritas Operations Manager helps you manage the user session timeout period for the Web server. Veritas Operations Manager lets you specify the timeout period in minutes. By default, the user session timeout period in Veritas Operations Manager is 30 minutes. If you want to disable the user session timeout period for the Web server, you must enter -1 in the Web server session timeout field.

See “Configuring the Web server settings in Veritas Operations Manager” on page 32.

Configuring the Web server settings in Veritas Operations Manager

In the Management server Settings view, you can set following:

- Log levels for all the log files that are created in the Web server.
- Timeout period for the Web server session.

You must enter the following details to set the log levels for all the log files:

<table>
<thead>
<tr>
<th>Log level</th>
<th>Select the log level that you want to set for all the log files in the Web server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You can select the following options:</td>
</tr>
<tr>
<td>Severe</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td></td>
</tr>
<tr>
<td>Debug</td>
<td></td>
</tr>
</tbody>
</table>

By default, Veritas Operations Manager set the log level as Info.
Enable log roll over

Specify whether you want to allow log roll over in Veritas Operations Manager. If you select No, the logs for a particular session are removed at the end of the session. If you select Yes, logs for all the sessions are added together to let you access a cumulative log record.

By default, Veritas Operations Manager displays No in this field.

To enable the timeout period for the Web server, you must enter the timeout period in minutes. By default, the timeout period for the Web server is 30 minutes. To disable the Web server timeout, you must enter -1 in the Web server session timeout field.

To configure the Web server settings in Veritas Operations Manager

1. In Veritas Operations Manager console, select Settings > Management Server.
2. In the Management Server Settings view, under Web Server Settings, enter the details and click Save Settings.

See “Viewing the Management Server settings” on page 28.

Viewing the details of active users logged in to Management Server

In the Settings > Management Server view, under Active Users, you can view the following information about active users logged in to Management Server:

- User name with which the active user has logged in to Management Server
- Date and time at which the user has logged in to Management Server
- The time for which the user was idle in Veritas Operations Manager
- Host name or IP address of the host from which the user logs in

To view the details of active users logged in to Management Server

1. In Veritas Operations Manager console, select Settings > Management Server.
2. In the Management Server Settings view, under Active Users, view the details of the active users who have logged in to Management Server.

See “Viewing the Management Server settings” on page 28.
Configuring Management Server settings

Viewing the details of active users logged in to Management Server
Managing Veritas Operations Manager alerts

This chapter includes the following topics:

■ About faults and risks
■ Viewing faults and risks
■ About analyzing faults
■ Analyzing faults in Veritas Operations Manager
■ Suppressing faults
■ Viewing the faults definitions
■ Suppressing the fault definitions
■ Activating suppressed fault definitions
■ Activating suppressed faults
■ About alerts
■ About alert rules
■ Viewing alert rules
■ Creating alert rules
■ Viewing the overview of a rule
■ Modifying alert rules
■ Copying alert rules
About faults and risks

Veritas Operations Manager enables you to view all possible problems in the environment that it manages at several levels in the user interface.

You can monitor the faulty status and possible risks to the managed resources and also analyze each fault to understand its implications and causes. You can also automate error handling by developing rules that trigger specific actions in response to alert conditions.

Faults in the SFHA environment are hierarchical in nature. For example, a fault on the disk causes a fault on the related volume, which in turn, causes a fault in the VCS resource managing it. Hence, it is very easy to identify the source of the fault using Veritas Operations Manager.

Faults are displayed in the following Veritas Operations Manager views:

- **Faults view**: Lists all the faulted entities in the managed environment along with fault source, time and cause.
- **Individual object detail view**: Indicates the possible cause, source, and time of the fault. It also indicates the objects's association with the business entity that is also impacted.
- **Business entities view**: Indicating all the faults for the business entity, possible causes, source, and time of the fault.

Veritas Operations Manager fault and risk monitoring answers the following types of questions:

- What are the conditions of the managed entities (applications, storage enclosures, hosts, clusters and so on) in the environment?
What are some of the possible causes of the fault?
What is the source of the fault?
What was the time when the fault occurred?
Are there any critical connections that are disabled?
How much space remains on critical storage?

Viewing faults and risks

On **Faults and Risks** page, you can view the system identified fault conditions along with their corresponding faulty entities and the fault sources. If required, you can suppress one or more faults for a specific period using the **Suppress Faults** option. You can also create rules for a selected fault. The rule determines the action that Veritas Operations Manager performs when it receives the alert that is related to a faulty entity. Click the **Analyze** icon to view the **Fault dependency view** panel that displays the hierarchy of a particular fault. You must have administrative privileges to create rules and suppress faults.

Using the provided search filter, you can search existing faults based on various criteria. For example, suppress status of the fault, type of the fault, type of the faulty entity and the storage type. Since it is dynamic search, the displayed fault list changes automatically as you type the term in the **Search** text box or when you select the check box for faulty entities. For instance, when you select **Exchange** check box in **Faulted Entity Type**, the application displays a list of only those faulty entities where Microsoft Exchange Server is installed. Similarly, when you select **Show only base faults** check box in **Fault type**, Veritas Operations Manager displays a list of only the base faults.

To view faults and risks

1. In Veritas Operations Manager console, select **Monitor > Faults**.
2. On the left panel, in **Search** text box, type the name of the fault that you want to search.
   - Click **Show all Faults and Risks** to view the list of all faults.

See “**About analyzing faults**” on page 37.
See “**Analyzing faults in Veritas Operations Manager**” on page 38.

About analyzing faults

Following data is displayed about the faults and risks in the managed objects by the Veritas Operations Manager interface:
Fault hierarchy: A graphical view shows the hierarchy of faults with severities associated with each fault. You can click on each fault to change the display on the right pane and provide more information on the selected fault.

Fault details: A detailed message about the fault, the time of the fault, the logs related to each object (if available), the associated alert, and the suppressed information on each fault.

Possible causes and related faults: A list of possible causes that created the fault. You can also add more causes that are specific to your environment for each fault ID.

Possible troubleshooting recommendations: A list of actions defined for each fault ID. These actions link to live pages to perform the remedial action. You can add remedial actions specific to your environment to each fault ID.

Links to UMI/SORT

Root cause analysis tool

## Analyzing faults in Veritas Operations Manager

Veritas Operations Manager lets you analyze faults that are reported on storage objects.

After you analyze a fault, you can view the following details in the Fault dependency view panel:

- Name of the entity where the fault occurred.
- Type of the faulted entity.
- Possible cause of the fault.
- Source of the fault.
- Date and time at which the fault occurred.

Also, the Fault dependency view panel gives you a graphical representation of the dependencies of the faulted entity.

In Veritas Operations Manager, you can analyze faults from the Faults and Risks view.

Also, you can analyze faults from the Overview view of the following storage objects:

- Business entities
- Hosts
- Disks
To analyze faults from the Faults and Risks view
1 In the Veritas Operations Manager console, select Monitor > Faults.
2 In the Faults and Risks view, in the Faulted Conditions table, select the corresponding check box of the fault that you want to analyze.
3 In the Faulted Conditions table, click the Analyze icon to display the details in the Fault dependency view panel.

To analyze faults from the details view of the storage objects
1 In the Veritas Operations Manager console, select Manage > Storage object.
   For example, to analyze faults from the Business Entities view, select Manage > Business Entities.
2 Click the name of the storage object to display the details view.
   For example, in the Business Entities view, click the name of a business entity to display the details view.
3 In the Overview view of the storage object, in the Faulted Conditions table, select the fault that you want to analyze.
   For example, in the Overview view of the business entity, in the Faulted Conditions table, select the fault that you want to analyze.
4 Do one of the following to display the details in the Fault dependency view window:
   ■ At the top of the Faulted Conditions table, click Analyze all faults.
   ■ In the Faulted Conditions table, right-click to select the fault that you want to analyze. From the shortcut menu, select Analyze all faults.

See “Viewing faults and risks” on page 37.
Suppressing faults

You can suppress one or more faults and fault definitions in Veritas Operations Manager. The following features are provided for the fault suppression management:

■ Ability to temporarily hide one or more faults.
■ Ability to disable the selected faults for the affected fault sources.
■ Ability to disable all the faults for the affected fault sources.
■ Ability to disable the fault definition itself.

For all the options, you can either specify the date and time to keep the faults in the suppressed state, or you can suppress the faults forever.

When you disable a fault definition, Veritas Operations Manager does not detect its corresponding faults. However, after you activate the fault definition, Veritas Operations Manager again uses that fault definition for subsequent fault detection.

You must have administrator rights to suppress the faults.

To suppress a fault

1  In the Veritas Operations Manager console, select Monitor > Faults.

2  In the Faults and Risks view, under Faulted Conditions table, select the fault that you want to suppress, and then do one of the following:
   ■ Click Suppress Faults.
   ■ Right-click the fault and from the submenu, select Suppress Faults.

3  On the Suppress Faults wizard panel, enter the required information and click OK.

    See “Suppress the Faults options” on page 40.

See “Analyzing faults in Veritas Operations Manager” on page 38.

See “Activating suppressed faults” on page 44.

Suppress the Faults options

Use this panel to suppress the faults in Veritas Operations Manager. You can hide or disable the faults either temporarily or permanently. You can disable a fault for a specific object; however, the fault definition is still considered as active for other objects.

For all these options, you can either specify the date and time to keep the faults in the suppressed state, or suppress the faults forever.
Table 3-1  Suppress Faults

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide the selected fault(s). Show again if the problem reoccurs.</td>
<td>Select this option to temporarily hide the selected fault. It is essentially hiding the current instance of the fault. The fault is displayed again when it is detected.</td>
</tr>
<tr>
<td>Disable the selected fault(s) for the affected fault sources</td>
<td>Select this option to disable the fault for the affected fault source.</td>
</tr>
<tr>
<td>Disable all fault(s) for the affected fault sources</td>
<td>Select this option to disable all faults for the affected fault source.</td>
</tr>
<tr>
<td>Hide or disable forever</td>
<td>Select this option to hide the fault without specifying any time interval.</td>
</tr>
<tr>
<td>Hide or disable until:</td>
<td>You can specify the date until which the fault remains suppressed. After this date, the fault is again considered as active in Veritas Operations Manager.</td>
</tr>
<tr>
<td>Reason</td>
<td>Provide the reason why the fault was suppressed. You can enter up to 254 characters for the description.</td>
</tr>
</tbody>
</table>

See “Suppressing faults” on page 40.

Viewing the faults definitions

You can view a comprehensive list of all the fault definitions that Veritas Operations Manager uses to generate all faults. You can use this list to view the definitions of the faults that are already generated and yet to generate. If you do not want to view a particular fault at all, you can disable its fault definition itself using the Suppress Faults option. After the fault definition is disabled, all associated faults are automatically suppressed. You can suppress the fault definition until a specific date, or disable it forever.

**Note:** Though the option to forever disable a fault definition is provided, you can again activate the fault definition using the Unsuppress Faults option.

Review the following information on this page:

- Type: Displays the type of the fault. For example, fault or risk.
- Message: Displays the information about the fault.
- Entity type: Displays the source object on which the fault has occurred.
- Affected Types: Displays all the object types that are affected by the fault on the source object. For example, if a service group (source object) is faulted, it is listed under the Entity Type column. Since a service group is associated with managed hosts, clusters, and other objects, Veritas Operations Manager generates derived faults for these objects. All such associated objects are listed in this column.

To view the faults definitions
- In Veritas Operations Manager console, select Monitor > Fault Definitions.

Suppressing the fault definitions

You can suppress the fault definitions for the faults that you want to disable permanently. After the definition itself is suppressed, Veritas Operations Manager treats the corresponding faults as non-existing. You can specify a period to keep the selected fault definition in the suppressed state.

Note: Though the option to forever disable a fault definition is provided, you can again activate the fault definition using the Unsuppress Faults option.

To suppress a fault definition

1. In the Veritas Operations Manager console, select Monitor > Fault Definitions.
2. In the Fault Definitions view, select the fault definition that you want to suppress, and do one of the following:
   - Click Suppress Faults.
   - Right-click the fault definition and from the submenu, select Suppress Faults.
3. On the Suppress Faults wizard panel, enter the required information and click OK.

See “Suppress the fault definition options” on page 43.
Suppress the fault definition options

Use this panel to suppress the selected fault definition. After the fault definition is suppressed, it is no longer displayed on Veritas Operations Manager user interface. You can suppress one or more fault definitions simultaneously.

Table 3-2 Suppress Faults

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide or disable forever</td>
<td>Select this option to disable the fault definition without specifying any time period.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Though the fault definition is suppressed forever, you can still activate it. This option provides additional flexibility to the users who want to be able to suppress the definition without specifying date along with the ability to re-activate the definition.</td>
</tr>
<tr>
<td>Hide or disable until:</td>
<td>You can specify the date until which the fault definition remains suppressed. After this date, the fault definition is again considered as active in Veritas Operations Manager.</td>
</tr>
<tr>
<td>Reason for hiding or disabling:</td>
<td>Provide the reason to suppress this fault definition. You can enter up to 254 characters for the description.</td>
</tr>
</tbody>
</table>

See “Suppressing the fault definitions” on page 42.

Activating suppressed fault definitions

You can activate a suppressed fault definition using Veritas Operations Manager console. After re-activation, Veritas Operations Manager starts using the fault definition for subsequent fault detections.

To activate a suppressed fault definition

1. In the Veritas Operations Manager console, select **Monitor > Faults Definitions**.

2. In the **Fault Definitions** view, select the suppressed fault definition that you want to activate, and do one of the following:
   - Click **Unsuppress Faults**.
Right-click the suppressed fault definition and from the submenu, select **Unsuppress Faults**.

3. On the **Unsuppress Faults** wizard panel click **OK**.

See “Activate the suppressed fault definition options” on page 44.

---

**Activate the suppressed fault definition options**

Use this panel to activate a suppressed fault definition. After the fault definition is activated, Veritas Operations Manager starts generating faults for this fault definition. You can activate more than one fault definitions simultaneously.

See “Activating suppressed fault definitions” on page 43.

---

**Activating suppressed faults**

You can activate the fault that is suppressed in Veritas Operations Manager.

When you suppress a fault, you set a date until which the fault is suppressed. After the specified date, the fault is again considered as active in the system. However, the Veritas Operations Manager also provides you with the option to activate the fault before that set date.

**To activate a suppressed fault**

1. In the Veritas Operations Manager console, select **Monitor > Faults**.

2. In the **Faults and Risks** view, under **Faulted Conditions** table, select the suppressed fault that you want to activate, and click **Unsuppress Faults**.

3. In the **Unsuppress Faults** panel, click **OK**.

See “Suppressing faults” on page 40.

---

**About alerts**

You can monitor the faulty status and performance information of your datacenter environment by reviewing alert notices on the Veritas Operations Manager Console. You can also automate error handling by developing rules that trigger specific actions in response to alert conditions.

You can set alert notices to show warnings about events and conditions, such as stopped replication or storage capacity, enabled or disabled I/O paths, faulted clusters and so on. These enable the administrator to make decisions about his environment and the resources managed by Veritas Operations Manager.
You can create rules which trigger actions in response to specific alerts or classes of alerts. You can also create rules which are based on alert severity level, topic or just the alert names, that can trigger one or more actions in response to specific alerts or classes of alerts.

Alerts can trigger actions such as sending emails to operators, displaying console alerts, sending an SMTP trap, or executing shell scripts and command files.

Veritas Operations Manager alerts provide answers to the following type of questions:

- What are the conditions of the managed entities (applications, storage enclosures, hosts, clusters and so on) in the environment?
- Are there any critical connections that are disabled?
- How much space remains on critical storage?

The alert severities that categorize the level of error are:

- Critical
- Error
- Warning
- Information

### About alert rules

Operators need to manage the condition of the resources in the environment. Operators typically define the custom rules that specify what conditions generate an alert, what actions should occur if an alert is detected, and which actions generate which type of alert severity. With Veritas Operations Manager, you can create and maintain rules pertaining to alerts.

When an alert is raised, the Veritas Operations Manager evaluates alert properties (alert name, severity, and classification). If an alert meets the conditions of a rule, the Veritas Operations Manager invokes one or more user-defined actions that are associated with the rule.

If an alert condition occurs, you can specify that Veritas Operations Manager initiate one of the following types of actions:

- Send an email message. For some alert conditions, operators may want to send emails notifying key personnel about the condition.
- Send an SNMP trap notification. Some objects are not polled. When events take place, these objects send traps or unsolicited asynchronous SNMP messages to the Server. Some of the rules that Veritas Operations Manager
uses to monitor objects in the environment rely on SNMP trap-based messages. The default port for the trap is 162.

- Execute a command script. For example, if an operator sees an alert that indicates that a switch is down or that it carries a high volume of traffic, the operator might execute a script that changes DMP paths so that key applications can bypass the problem switch.
- Upload a custom script and execute it. This facility provides the administrator more control over Veritas Operations Manager.

**Note:** You must provide the details for the SMTP settings and save them to the database before you set up the email notification for an alert using that SMTP settings. You can save the SMTP settings on the **Settings > Management Server** view.

With Veritas Operations Manager, you can create rules and do the following on rules you or anyone else created:

- Create rules.
- Edit rules that include renaming, enabling, and disabling rules.
- Delete rules.
- Copy rules.
- Enable rules.
- Disable rules.

**Note:** You must have administrator privileges to create, copy, view, or manage alert rules.

See “Viewing alert rules” on page 46.

See “Creating alert rules” on page 47.

# Viewing alert rules

**To view rules**

1. Select **Monitor > Rules**.
2. In the **Rule Manager** view, view the list of rules that you or anyone else created.
Creating alert rules

In Veritas Operations Manager you can create the rules that trigger various actions based on alert conditions. Aside from creating rules from the rules option, you can also create rules for selected faults and alerts.

This section explains creating rules in Veritas Operations Manager.

To create a rule from the Rules view

1. In the Veritas Operations Manager console, click Monitor > Rules.

2. In the Rules view, at the top of the Rules table, click the Create Rule tab.

3. In the Create Rule dialog box, select from the following options to create a rule, and click Next:
   - You can create a rule by selecting the alert condition that triggers an action.
   - You can create a rule by selecting the alert severity level.
   - You can also create a rule by selecting from a list of alert topics.
   See “Create Rule - Alert Conditions options” on page 48.

4. In the dialog box to select the source of the alert trigger, select if you want to trigger the rule for alerts originating from any host in the domain or specific hosts. Click Next.
   See “Create Rule - Trigger Alert Source options” on page 50.

5. In the wizard panel to specify the notification medium, select the required option. Click Next.
   See “Create Rule - Setup notifications options” on page 50.

6. In the wizard panel to specify the descriptions for the rule, enter the required information. Click Finish

7. See “Create Rule - Description” on page 53.

8. In the Result panel, verify that the rule has been successfully created.

To create a rule from the Faults and Risks view

1. In the Veritas Operations Manager console, click Monitor > Faults.

2. From the Faulted Conditions table, select the fault for which you want to create the rule.

3. Click Create Rule.

4. In the Create Rule panel, enter the alert that triggers actions for the rule that you create. Click Next.
   See “Create Rule - Alert Conditions options” on page 48.
5 In the wizard panel to specify the alert source, select the required option. Click **Next**.

See “Create Rule - Trigger Alert Source options” on page 50.

6 In the wizard panel to specify the notification medium, select the required option. Click **Next**.

See “Create Rule - Setup notifications options” on page 50.

7 In the wizard panel to specify the descriptions for the rule, enter the required information. Click **Finish**

See “Create Rule - Description” on page 53.

8 In the **Result** panel, verify that the rule has been successfully created.

**To create a rule from the Alerts view**

1 In the Veritas Operations Manager console, click **Monitor > Alerts**.

2 From the **Alerts** table, select the alert for which you want to create a rule.

3 Click **Create Rule**.

4 In the **Create Rule** panel, enter the alert that triggers actions for the rule that you create. Click **Next**.

See “Create Rule - Alert Conditions options” on page 48.

5 In the wizard panel to specify the alert source, select the required option. Click **Next**.

See “Create Rule - Trigger Alert Source options” on page 50.

6 In the wizard panel to specify the notification medium, select the required option. Click **Next**.

See “Create Rule - Setup notifications options” on page 50.

7 In the wizard panel to specify the descriptions for the rule, enter the required information. Click **Finish**

See “Create Rule - Description” on page 53.

8 In the **Result** panel, verify that the rule has been successfully created.

See “About alert rules” on page 45.

See “Modifying alert rules” on page 54.

**Create Rule - Alert Conditions options**

Use this panel to define the context and conditions of an alert that triggers an automatic action.
Table 3-3 refers to possible alert condition options that you can select to create a rule.

Table 3-3  
Create Rule - Alert Conditions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| This rule will be triggered for all alerts with a severity of | Select this option to trigger this rule for any alerts with the selected severity. Each alert is assigned a severity level upon creation. You can set the rule to trigger the automatic action for all alerts with a specific severity level. You can select the following severity levels for the alert:  
  - Critical  
  - Error  
  - Warning  
  - Information  
The default severity is Critical. |
| Enter the alert(s) that will trigger the action(s) for this rule | Select this option to trigger the rule when the specifically entered alert ID(s) occur. Each alert is assigned an alert ID upon creation. You can set the rule to trigger the automatic action for all alerts with a specific alert ID. Use semicolon (;) to separate multiple entries. |
| Choose from a list of alerts | Select this option to trigger this rule when specific alerts occur. Click Next > to display a list of all alert topics and classifications that are available. |

See “Creating alert rules” on page 47.

Create Rule - Select Alerts options

Use this panel to select the specific alerts that will trigger this rule. Select the alerts from the table. The table contents reflect the filtering selections made in the Create Rule - Alert Conditions panel.

See “Creating alert rules” on page 47.
Create Rule - Trigger Alert Source options

Use this dialog box to select the specific alert sources that triggers this rule. 
Table 3-4 refers to possible Trigger Alert Source options that you can select to create a rule.

Table 3-4 Create Rule - Trigger Alert Source options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Rule for alerts originating from any host in the domain</td>
<td>Select this option to activate the rule when the designated alert occurs on any monitored host in the domain. This is the default selection.</td>
</tr>
<tr>
<td>Trigger rule for alerts originating from specific hosts</td>
<td>Select this option to activate the rule when the designated alert occurs on specific hosts in the domain. To specify the host, check the name of the host. You can also filter the list of the hosts.</td>
</tr>
</tbody>
</table>

See “Creating alert rules” on page 47.

Create Rule - Setup notifications options

Use this wizard panel to set up notifications for the rule. You can check any or all of the following check boxes to set up the notification:

**Note:** You can choose multiple notification options. For all the notifications methods that you have selected, fill in the required information.

<table>
<thead>
<tr>
<th>Email</th>
<th>Check to set up an email notification when the alert conditions that are specified by the rule occur.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap</td>
<td>Check to send an SNMP Trap when the alert conditions that are specified by the rule occur.</td>
</tr>
<tr>
<td>Command script</td>
<td>Check to run a command script when the alert conditions that are specified by the rule occur.</td>
</tr>
</tbody>
</table>
Check to run a custom script when the alert conditions that are specified by the rule occur.

You must set up at least one type of notification for the rule that you create.

**Table 3-5**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Email: To      | Enter the email address of one or more users or groups that you want Management Server to notify. Separate the multiple entries with a comma (.). Visible only when email is selected.  
Example: 123@example.com, 456@example.com                                                                 |
| Email: Email Format | Displays the email body format. Not Editable. Variables, indicated by the words in brackets, are replaced by the specific alert information indicated.  
[Rule Name] = The name of the rule that is specified in the first dialog box.  
[Severity Level] = The severity of the alert. For example, Critical.  
[Description] = The detail description for the alert. Set by the alert.  
[Action] = The recommended action that should be done for the alert.  
[Source Host] = The host where the alert originated.  
[Alert Classification] = The classification of the alert. Set by the alert.  
[Alert Name] = The name of the alert. Set by the alert.  
[Alert Date And Time] = The timestamp when the alert was first created on the source host. |
### Table 3-5 (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email: Send email as daily digest</td>
<td>Check to send the email notification as daily digest. If you check this check box, SF Manager combines all your email alert notifications into one summary email and sends to you everyday.</td>
</tr>
<tr>
<td>SNMP Trap: Host</td>
<td>Enter the IP Address or name of the host where the SNMP trap console is located. Visible only when SNMP Trap is selected. Example: Host123.example.com</td>
</tr>
<tr>
<td>SNMP Trap: Port</td>
<td>Displays the port number 162, the default port number for SNMP traps. You can edit the port number, if required.</td>
</tr>
<tr>
<td>Command Script: Source Host</td>
<td>Enter the name of the host where the command script file is located. Maximum length is 255 characters. The source host name cannot contain spaces. Example: Host123.example.com</td>
</tr>
<tr>
<td>Command Script: Source File</td>
<td>Enter the path and name of the command script file. Maximum length is 255 characters. Valid entries should contain the full path and a valid file name. Visible only when Command script is selected. Example: /opt/scripts/script1.exe</td>
</tr>
<tr>
<td>Command Script: Destination host</td>
<td>Enter the name of the host where the command script file is to be executed. Maximum length is 255 characters. The destination host name cannot contain spaces. Accepts multiple entries that are separated by comma(.). Example: Host456.example.com</td>
</tr>
</tbody>
</table>
Table 3-5  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Custom script: Custom script | Browse the custom script file and upload it. You can only upload the following types of scripts:  
|                           | ■ perl (.pl)                                                                |
|                           | ■ shell (.sh)                                                                |
|                           | ■ batch (.bat)                                                               |

See “Creating alert rules” on page 47.

Create Rule - Description

Use this panel to assign a name and description to a new rule. Rules define the automatic actions taken when specific alerts are generated, and they are listed on the Rule Manager tab.

For example, a rule can automatically run a script to restart an application when it receives an alert saying that the application has stopped. This allows network administrators to automate routine tasks and focus their energies on more critical issues.

Table 3-6  Create Rule - Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Rule Name | Enter the name of the rule. Maximum field length is 255 characters.  
|          | Example: Restart stopped ABC program.                                       |
| Description | Enter a description for this rule. The description should include the purpose of the rule. Maximum field length is 255 characters. Example: When the ABC program generates a service stopped alert, run the restart program script and send an alert to the SNMP trap console. |
| Enable Rule | Uncheck to disable the rule. The default is enabled. An enabled rule monitors alerts for the defined conditions. |

See “Creating alert rules” on page 47.
Viewing the overview of a rule

The Rule page displays the properties of the selected rule. The information on this page includes:

- **Overview**: It includes name of the rule, its description, its current state, name of the owner, and the date when the rule was last modified.

- **Alert Conditions**: It includes the alert conditions that are configured for this rule.

- **Actions**: It displays the actions the system performs when a rule is executed. The information includes E-mail notification details, SNMP configuration, command file details, and the information about custom script.

You can create rules for faults as well as alerts from their respective user interface panels. All such rules are also displayed on this page.

To view the overview for a rule

1. In the Veritas Operations Manager console, select **Monitor > Rules**.
2. Click the rule that you want to overview.

See “Creating alert rules” on page 47.

See “Modifying alert rules” on page 54.

See “Disabling alert rules” on page 63.

Modifying alert rules

In Veritas Operations Manager, you can modify an alert rule that you have created. You can modify the following elements of an alert rule:

- Alert condition
- Alert source
- Notification method
- Name and description

You can modify the alert rule from the following views:

- Rule Manager view
- Details view of the individual alert

You must have administrator privilege to modify an alert rule.
To modify a rule

1  In the Veritas Operations Manager console, click Monitor > Rule.

2  In the Rules table, click the name of the rule that you want to modify and do one of the following:
   ■  Click Edit Rule.
   ■  In the Overview view of the rule, Click Edit Rule.

3  In the panel to define alert condition, modify the alert condition that triggers an action and then do one of the following:
   ■  Click Next to continue.
   ■  Click Finish to exit the wizard. You cannot perform the rest of the steps mentioned below. However, you can edit the rule again to perform these steps.

See “Edit Rule - Alert Conditions options” on page 56.

4  If you chose the multiple alerts condition in step 4, in the Edit Rule - Select Alerts panel, check one or more alerts in the table and then do one of the following:
   ■  Click Next to continue.
   ■  Click Finish to exit the wizard. You cannot perform the rest of the steps mentioned below. However, you can edit the rule again to perform these steps.

See “Edit Rule - Select Alerts options” on page 57.

5  In the Edit Rule - Trigger Alert Source panel, modify the selection of the required alert source and then do one of the following:
   ■  Click Next to continue.
   ■  Click Finish to exit the wizard. You cannot perform the rest of the steps mentioned below. However, you can edit the rule again to perform these steps.

See “Edit Rule - Trigger Alert Source options” on page 57.

6  In the Edit Rule - Setup notifications panel, modify the notifications that you have specified for the rule and do one of the following:
   ■  Click Next to continue.
   ■  Click Finish to exit the wizard. You cannot perform the rest of the steps mentioned below. However, you can edit the rule again to perform these steps.
See “Edit Rule - Setup notifications options” on page 58.

7 In the Edit Rule - Name panel, modify the details of the rule and then do one of the following:

■ Click Next to continue.
■ Click Finish to exit the wizard.

See “Edit Rule - Name options” on page 60.

8 In the Result panel, verify that the rule has been successfully modified. Click OK.

You can view the modified rule listed in the Rules table. If you elected to enable the rule immediately, the rule is followed as soon as its conditions are met.

See “About alert rules” on page 45.
See “Disabling alert rules” on page 63.
See “Enabling alert rules” on page 62.

### Edit Rule - Alert Conditions options

Use this panel to define the context and conditions of an alert that triggers an automatic action.

**Table 3-7  Edit Rule - Alert Conditions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This rule will be triggered for all alerts with a severity of</td>
<td>Select this option to trigger this rule for any alerts with the selected severity. Each alert is assigned a severity level upon creation. You can set the rule to trigger the automatic action for all alerts with a specific severity level. You can modify the severity level for the alert by selecting any of the following:</td>
</tr>
<tr>
<td></td>
<td>■ Critical</td>
</tr>
<tr>
<td></td>
<td>■ Error</td>
</tr>
<tr>
<td></td>
<td>■ Warning</td>
</tr>
<tr>
<td></td>
<td>■ Information</td>
</tr>
<tr>
<td></td>
<td>The default severity is Critical.</td>
</tr>
</tbody>
</table>
Table 3-7  Edit Rule - Alert Conditions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the alert topic(s) that</td>
<td>Enter the alert topics that trigger the actions for this rule. If you enter</td>
</tr>
<tr>
<td>will trigger the action(s) for</td>
<td>multiple topics, you must separate each topic with a semi-colon.</td>
</tr>
<tr>
<td>this rule (separated by ';'</td>
<td></td>
</tr>
<tr>
<td>Choose from a list of alerts</td>
<td>Select this option to trigger the rule when specific alerts occur. Click</td>
</tr>
<tr>
<td></td>
<td><strong>Next</strong> to display a list of all alert topics and classifications that are</td>
</tr>
<tr>
<td></td>
<td>available, optionally filtered according to these criteria:</td>
</tr>
<tr>
<td></td>
<td>■ Severity: Check to filter the alerts based on severity level. Select</td>
</tr>
<tr>
<td></td>
<td>the filter’s severity level from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>■ Topic: Check to filter the alerts based on the entered topic. Enter</td>
</tr>
<tr>
<td></td>
<td>the text for the filter to sort the topics. You can enter partial text</td>
</tr>
<tr>
<td></td>
<td>to view all alert conditions with the partial text in the topic field.</td>
</tr>
<tr>
<td></td>
<td>Wildcard characters, such as an asterisk (*), or multiple word entries are</td>
</tr>
<tr>
<td></td>
<td>not valid.</td>
</tr>
</tbody>
</table>

See “Modifying alert rules” on page 54.

Edit Rule - Select Alerts options

Use this panel to select the specific alerts that will trigger this rule. Select the alerts from the table. The table contents reflect the filtering selections made in the **Edit Rule - Alert Conditions** panel.

Check the **Include VEA alert topics** check box to include the alerts specific to Veritas Enterprise Administrator.

See “Modifying alert rules” on page 54.

Edit Rule - Trigger Alert Source options

Use this panel to select the specific alert sources that triggers the rule.

Table 3-8  Edit Rule - Trigger Alert Source

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Rule for alerts originating from any host in the</td>
<td>Select this option to activate the rule when the designated alert occurs</td>
</tr>
<tr>
<td>domain</td>
<td>on any monitored host in the domain. This is the default selection.</td>
</tr>
</tbody>
</table>
### Edit Rule - Trigger Alert Source (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger rule for alerts originating from specific hosts</td>
<td>Select this option to activate the rule when the designated alert occurs on specific hosts in the domain. To specify the host, check the name of the host. You can also filter the list of the hosts.</td>
</tr>
</tbody>
</table>

See “Modifying alert rules” on page 54.

### Edit Rule - Setup notifications options

Use this wizard panel to modify the notifications that you set up for the selected rule. You can check any or all of the following check boxes to modify the notification setup:

- **Email**: Check to modify the email notification.
- **SNMP Trap**: Check to modify the SNMP Trap.
- **Command Action**: Check to modify the command action.
- **Custom script**: Check to modify the custom script that you have specified.

### Table 3-9

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email</strong></td>
<td></td>
</tr>
<tr>
<td><strong>To</strong></td>
<td>Enter the email address of one or more users or groups that you want the Management Server to notify. Separate multiple entries with comma (,). Visible only when email is selected. Example: <a href="mailto:123@example.com">123@example.com</a>; <a href="mailto:456@example.com">456@example.com</a></td>
</tr>
</tbody>
</table>
Table 3-9  Edit Rule - Setup notifications options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Format</td>
<td>Displays the email body format. Not Editable. The specific alert information replaces the variables that are indicated in brackets in the following list:</td>
</tr>
<tr>
<td></td>
<td>- [Rule Name] = The name of the rule that is specified in the first dialog box.</td>
</tr>
<tr>
<td></td>
<td>- [Severity Level] = The severity of the alert. For example, Critical.</td>
</tr>
<tr>
<td></td>
<td>- [Description] = The detail description for the alert. Set by the alert.</td>
</tr>
<tr>
<td></td>
<td>- [Action] = The recommended action that should be done for the alert.</td>
</tr>
<tr>
<td></td>
<td>- [Source Host] = The host where the alert originated.</td>
</tr>
<tr>
<td></td>
<td>- [Alert Classification] = The classification of the alert. Set by the alert.</td>
</tr>
<tr>
<td></td>
<td>- [Alert Name] = The name of the alert. Set by the alert.</td>
</tr>
<tr>
<td></td>
<td>- [Alert Date And Time] = The timestamp when the alert was first created on the source host.</td>
</tr>
<tr>
<td>Send email as daily digest</td>
<td>Check to send the email notification as daily digest. If you check this check box, SF Manager combines all your email alert notifications into one summary email and sends to you everyday.</td>
</tr>
</tbody>
</table>

**SNMP Trap**

<table>
<thead>
<tr>
<th>Host</th>
<th>Enter the IP Address or the name of the host where the SNMP trap console is located. Visible only when SNMP Trap is selected. Example: Host123.example.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Displays the port number 162, the default port number for SNMP traps. You can edit the port number, if required.</td>
</tr>
</tbody>
</table>
Table 3-9  Edit Rule - Setup notifications options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Action</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Source Host</strong></td>
<td>Enter the name of the host where the command script file is located. Maximum length is 255 characters. The source host name cannot contain spaces.</td>
</tr>
<tr>
<td></td>
<td>Example: Host123.example.com</td>
</tr>
<tr>
<td><strong>Source File</strong></td>
<td>Enter the path and name of the command script file. Maximum length is 255 characters. Valid entries should contain the full path and a valid file name. Visible only when Command script is selected.</td>
</tr>
<tr>
<td></td>
<td>Example: /opt/scripts/script1.exe</td>
</tr>
<tr>
<td><strong>Argument List</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Destination host</strong></td>
<td>Enter the name of the host where the command script file is to be executed. Maximum length is 255 characters. The destination host name cannot contain spaces. Use comma (,) to separate the multiple host name entries.</td>
</tr>
<tr>
<td></td>
<td>Example: Host456.example.com</td>
</tr>
<tr>
<td><strong>Custom script</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Custom script</strong></td>
<td>Browse the custom script file and upload it. You can only upload the following types of scripts:</td>
</tr>
<tr>
<td></td>
<td>■ perl (.pl)</td>
</tr>
<tr>
<td></td>
<td>■ shell (.sh)</td>
</tr>
<tr>
<td></td>
<td>■ batch (.bat)</td>
</tr>
</tbody>
</table>

See “Modifying alert rules” on page 54.

**Edit Rule - Name options**

Use this panel to edit the name and description for an existing rule. Rules define the automatic actions that are taken when specific alerts are generated, and they are listed on the **Rules** tab.
For example, a rule can automatically run a script to restart an application when it creates an alert that the application has stopped. This allows network administrators to automate routine tasks and focus their energies on more critical issues.

### Table 3-10 Edit Rule - Name

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Edit the name of the rule. Maximum field length is 255 characters. Example: Restart stopped ABC program.</td>
</tr>
<tr>
<td>Description</td>
<td>Edit the description for this rule. The description should include the purpose of the rule. Maximum field length is 255 characters. Example: When the ABC program generates a service stopped alert, run the restart program script and send an alert to the SNMP trap console.</td>
</tr>
<tr>
<td>Enable Rule</td>
<td>Uncheck to disable the rule. The default is enabled. An enabled rule monitors alerts for the defined conditions.</td>
</tr>
</tbody>
</table>

See “Modifying alert rules” on page 54.

### Copying alert rules

The administrators can copy rules and specify their properties. This option is more efficient than creating new rules.

#### To copy an alert rule

1. Click Monitor > Rules.
2. From the list of existing rules, select the rule that you want to copy, and do one of the following:
   - Click More > Copy Rule.
   - Right-click the desired rule and from the submenu, select Copy Rule.
3. In the Copy Rule wizard panel, specify the name of the new rule and click OK.

   See “Copy Rule options” on page 62.
4. In the Results panel click OK.

See “Creating alert rules” on page 47.

See “Modifying alert rules” on page 54.
See “Deleting alert rules” on page 64.
See “Disabling alert rules” on page 63.
See “Enabling alert rules” on page 62.

Copy Rule options

Use this panel to create an identical copy of the selected rule with a distinct name. After you create a copy of the original rule, you can edit its properties to make it unique.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of New Rule</td>
<td>Enter a name for the new rule.</td>
</tr>
</tbody>
</table>

See “Copying alert rules” on page 61.

Enabling alert rules

You can enable the alert rules that are in the disabled state. You can perform this task from any of the following views:

- Rule Manager view.
- Overview view of an alert rule.

Depending on the status of the alert rule that you have selected, the Overview page of the alert rule displays the Enable Rule option or the Disable Rule option.

To enable a rule

1. In the Veritas Operations Manager console, select Monitor > Rules.
2. From the list of existing rules, check the rule that you want to disable and do one of the following:
   - At the top of the Rules table, click the More drop-down list and select Enable Rule.
   - Click on the name of the rule to go to the Overview page. In the Overview page, click Enable Rule.
3. In the Enable Rule panel, click Yes.
4. In the Result panel, verify that the rule has been successfully enabled. Click OK.
Disabling alert rules

You can disable the alert rules that are in the enabled state. You can perform this task from any of the following views:

- Rule Manager view.
- Overview view of an alert rule.

Depending on the status of the alert rule that you have selected, the Overview view of the alert rule displays the Disable Rule option or the Enable Rule option.

To disable a rule

1. In the Veritas Operations Manager console, select Monitor > Rules.
2. From the list of existing rules, check the rule that you want to disable and do one of the following:
   - At the top of the Rules table, click More drop-down list and select Disable Rule.
   - Click on the name of the rule to go to the Overview page. In the Overview page, click Disable Rule.
3. In the Disable Rule panel, click Yes.
4. In the Result panel, verify that the rule has been disabled successfully. Click Ok.

See “About alerts” on page 44.
See “About alert rules” on page 45.
See “Viewing alerts” on page 64.
See “Creating alert rules” on page 47.
See “Modifying alert rules” on page 54.
Deleting alert rules

You can delete the alert rules that are no longer needed.

To delete an alert rule

1  Click Monitor > Rules.

2  From the list of existing rules, select the rule that you want to delete and do one of the following:
   ■  Click More > Delete Rule.
   ■  Right-click the desired rule and from the submenu, select Delete Rule.

3  In the Delete Rule wizard panel, click Yes.
   See “Delete an Existing Rule options” on page 64.

4  In the Results panel, click OK.
   See “Creating alert rules” on page 47.
   See “Copying alert rules” on page 61.
   See “Modifying alert rules” on page 54.
   See “Disabling alert rules” on page 63.
   See “Enabling alert rules” on page 62.

Delete an Existing Rule options

Use this panel to remove an existing rule. Deleted rules are no longer available for sending emails, generating SNMP traps, or executing command scripts in response to alerts.

See “Deleting alert rules” on page 64.

Viewing alerts

Operators monitor faulty status and performance information of the storage network by reviewing alert notices. Veritas Operations Manager alerts help operators answer the following types of questions:
What are the conditions of hosts, Initiators, disk groups, disks, or applications in the environment?

Are there any critical connections that are disabled?

How much space remains on critical storage?

Alerts show warnings about events and conditions, such as VxFS file system capacity monitoring, file system status, VxFS file system storage checkpoint alerts, VVR alerts, enabled or disabled paths, alternate paths available or not available, enabled or disabled disks, system I/O alerts, Action Provider alerts, and VxVM provider service alerts. These items show as alert classifications.

The following alert severities categorize the level of the error:

- Critical
- Error
- Warning
- Information

With the Veritas Operations Manager Console, operators can quickly ascertain the condition of all resources in the Veritas Operations Manager environment. The Alert Log displays alerts from all hosts that the central server manages.

Alert conditions can trigger actions such as sending emails to operators that inform them about alert conditions, sending an SMTP trap, or running a batch file on specific hosts.

Veritas Operations Manager retains Alert Logs for 30 days.

In the Alerts view, you can view the following information in a table:

- The message which is a part of the alert. It includes the name of the agent that identified the alert condition and the name of the host on which the alert condition occurred.
- The classification of the alert, for example, Volume alert, Subdisk alert, and path enabled.
- The host on which the alert condition occurred.
- The date and time when the alert was generated.
- The number of alerts.

You can view the detailed information about an alert by clicking on the icon in the Details column. The Alert Log Details panel displays the detailed information about an alert.

See “Alert Log Details options” on page 66.

You can use the options on the left-side panel to do the following:
Search for alerts based on message, classification, and source host.

Filter the tasks based on their severity.

To view all alerts

◆ In the Veritas Operations Manager console, select **Monitor > Alerts**.

**Alert Log Details options**

In this panel, you can view the details of an alert.

You can add a note regarding the alert in the **Alert Log Details** panel by clicking **Add Note**.

**Table 3-12** Alert Log Details panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Displays the alert level: Critical, Error, Warning, or Information.</td>
</tr>
<tr>
<td>Topic</td>
<td>Displays the alert name.</td>
</tr>
<tr>
<td>Date</td>
<td>Displays the date and time on which the alert was generated.</td>
</tr>
<tr>
<td>Message</td>
<td>Displays the message from the alert, usually including the name of the agent that identified the alert condition and the name of the host on which the alert condition occurred.</td>
</tr>
<tr>
<td>Class</td>
<td>Displays the alert classification, for example, Volume alert, Subdisk alert, and path enabled.</td>
</tr>
<tr>
<td>Host</td>
<td>Displays the host on which the alert condition occurred.</td>
</tr>
<tr>
<td>Recommended Action</td>
<td>Displays the recommended action to resolve the issue.</td>
</tr>
<tr>
<td>Details</td>
<td>Displays the details about the cause of the alert.</td>
</tr>
</tbody>
</table>
About tasks

A task represents any operation that can be performed by using Veritas Operations Manager. You can view the list of all tasks and the details about each of them in the Tasks view. The list of all tasks lets you keep a track of all the operations that are either in progress or that have completed for the various datacenter objects. See “Viewing tasks” on page 67.

Viewing tasks

In Veritas Operations Manager, you can view the list of tasks that are either in progress or that have completed. You can also view the tasks that have failed. You can view the following information about the tasks in a table:

- The name of the task.
- The state of the task: In Progress, Completed, or Failed.
- The target object on which the task must be executed.
- The system on which the task must be executed.
- The user that executes the task.
- The start time of the task.
- The end time of the task.
- The total number of tasks.

You can view the detailed information about a task by clicking on the icon in the Details column. The Task Details panel displays the detailed information such as the commands that are executed as part of the task and their results.

You can use the options on the left-side panel to do the following:

- Search for tasks based on task name, state, target, source, and user.
- Filter the tasks based on their current state.

To view the list of tasks

- In the Veritas Operations Manager console, select Monitor > Tasks.

See “About tasks” on page 67.
About messages posted on Activity Board

You can post messages in the Activity Board panel on the Veritas Operations Manager Home view. These messages let you inform other users about any administrative or other important activities that are scheduled or that may have been performed.

See “Viewing the messages posted on Activity Board” on page 68.

Viewing the messages posted on Activity Board

In Veritas Operations Manager, you can view all the messages that are posted on the Activity Board panel in the Veritas Operations Manager Home view. You can view only the 10 most recent messages on the Veritas Operations Manager Home view.

In the Activity Board view, you can view the following information in a table:

- The date and time at which the message was sent.
- The sender of the message.
- The message that was sent.

You can use the Search option on the left-side panel to search for messages based on the sender and the message.

To view all the messages posted on Activity Board

In the Veritas Operations Manager console, do one of the following:

- Select Monitor > Activities.
- In the Activity Board panel on the Home view, click Show all.

See “About messages posted on Activity Board” on page 68.

Deleting a message that is posted on Activity Board

In the Activity Board view of Veritas Operations Manager, you can remove the messages that are posted on the Activity Board panel.

To remove a message that is posted on Activity Board

1. In the Veritas Operations Manager console, select Monitor > Activities.
2. In the Activity Board view, in the All Activities table, select the checkbox to on the left-side of the message that you want to remove and do one of the following:
At the top of the All Activities table, click Delete Message(s).

Right-click the message that you want to remove and from the submenu, select Delete Message(s).

3 In the Delete Message(s) panel, click Yes to remove the message.

4 In the Results panel, click OK.

See “Viewing the messages posted on Activity Board” on page 68.
Managing Veritas Operations Manager alerts

Deleting a message that is posted on Activity Board
Deploying Veritas Operations Manager solutions

This chapter includes the following topics:

- About Veritas Operations Manager solutions
- About deploying Veritas Operations Manager solutions
- Viewing Veritas Operations Manager solutions in the repository
- Uploading a solution to repository
- Installing Veritas Operations Manager solution
- Upgrading managed hosts using Veritas Operations Manager console
- Uninstalling a solution
- Removing a Veritas Operations Manager solution from repository
- Viewing the solution deployment summary and the hosts to install solution
- Installing solutions on specific managed hosts
- Uninstalling solutions from specific managed hosts
- Enabling the solution on specific managed hosts
- Disabling the solution on specific managed host
- Viewing the deployment requests for a solution
- Canceling the deployment request for a solution
About Veritas Operations Manager solutions

Veritas Operations Manager solutions are independent and optional feature packs that you can download and use to enhance the functionality of Veritas Operations Manager. These solutions are grouped into the following categories:

- Add-on
- Package
- Patch
- Hotfix

The solutions can be installed on Veritas Operations Manager Management Server and the managed hosts. To deploy these solutions you must have domain administrative privileges. The status information for the solutions is maintained in the Management Server database.

See “About deploying add-ons” on page 73.

See “About deploying packages or patches” on page 75.

See “Installing Veritas Operations Manager solution” on page 78.

See “Downloading the deployment log for a solution’s deployment request” on page 88.

About deploying Veritas Operations Manager solutions

This section provides you with the required information to deploy solutions (add-on, package, patch, and hotfix) for Veritas Operations Manager.

After uploading a solution to the repository, you can install the solution on the Management Server, managed host or on both (whichever is applicable). You can install a solution on the selected hosts, or you can select a platform (for example AIX), and install the solution on all the managed hosts that use the specific platform. When you run the installation process, a deployment request is sent. You can view that deployment request in the Deployment Requests page. The following list provides an overview of various states of the solution that you see on the User Interface of Veritas Operations Manager:

- Upload: You need to upload the solution to the repository before you install it. Note that few solutions (add-ons) are pre-bundled with Veritas Operations
Manager. For those add-ons, you can directly proceed with the installation. You can download other add-ons from Symantec support Web site. When a solution is uploaded, it is in the Not Installed state. To use the solution, you need to install it on managed hosts, Management Server, or on both (whichever is applicable for the solution).

- **Install**: After you upload the solution, you need to install the solution before you can start using it. Once the solution is installed, you can enable or disable it.
- **Enable**: The solution must be in the installed state before you can enable it.
- **Disable**: The solution must be in the installed state before you can disable it.
- **Uninstall**: If the add-on is no longer used, you can uninstall it. After you have uninstalled it, enable and disable options are not available. However, even after uninstalling the add-on, it is still present in the repository. If required, you can again install it. Note that you can uninstall the solution irrespective of its state (enabled or disabled).
- **Remove**: You need to uninstall the solution (add-on or hotfix) before you can remove it. That is, the add-on must be in Not Installed state before you can remove it. You cannot remove the solutions, which are pre-bundled with Veritas Operations Manager.

See “About deploying add-ons” on page 73.

See “About deploying packages or patches” on page 75.

See “Uploading a solution to repository” on page 77.

See “Installing Veritas Operations Manager solution” on page 78.

**About deploying add-ons**

This section provides you with the list of Veritas Operations Manager add-ons (pre-bundled with the application). It also describes the required actions when you want to install these add-ons on the managed hosts.

For example, to administer a UNIX managed hosts from the Management Server, download and deploy Storage Foundation Administration for Unix Add-on on Management Server. To administer a Windows managed hosts from the Management Server, download and deploy Storage Foundation Administration for Windows Add-on on the Management Server. To enable template-based storage provisioning from Management Server, you must download and deploy Veritas Storage Foundation Add-on for Storage Provisioning on Management Server.

The following Veritas Operations Manager add-on is deployed along with the Management Server installation:
Add-ons and their supported versions in Veritas Operations Manager

The following table lists the add-ons that you need to download and deploy in Veritas Operations Manager. This table also lists the supported versions of these add-ons in Veritas Operations Manager 4.0:

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Supported versions in Veritas Operations Manager 4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Foundation Administration for Unix Add-on</td>
<td>4.0</td>
</tr>
<tr>
<td>Storage Foundation Administration for Windows Add-on</td>
<td>4.0</td>
</tr>
<tr>
<td>Note: To manage the Windows managed hosts using Veritas Operations Manager 4.0, you must install the 4.0 version of the VRTSsfmh package on them.</td>
<td></td>
</tr>
<tr>
<td>Veritas Operations Manager Add-on for Veritas Cluster Server User Password Management</td>
<td>4.0</td>
</tr>
<tr>
<td>Veritas Operations Manager Business Entity Operations Add-on</td>
<td>4.0</td>
</tr>
<tr>
<td>Veritas Operations Manager CommandCentral Storage Add-on</td>
<td>5.2.2116.0</td>
</tr>
<tr>
<td>Veritas Operations Manager Distribution Manager Add-on</td>
<td>3.1.201.0</td>
</tr>
<tr>
<td>Veritas Operations Manager LDom Capacity Management Add-on</td>
<td>4.0</td>
</tr>
<tr>
<td>Veritas Operations Manager Package Anomaly Add-on</td>
<td>4.0</td>
</tr>
<tr>
<td>Veritas Operations Manager Scripting Add-on</td>
<td>4.0</td>
</tr>
</tbody>
</table>
Table 4-1  Supported versions of Add-ons in Veritas Operations Manager 4.0 (continued)

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Supported versions in Veritas Operations Manager 4.0</th>
</tr>
</thead>
</table>
| Veritas Operations Manager Storage Insight Add-on for Deep Array Discovery and Mapping | 3.1.101.0  
3.1.201.0  
3.1.251.0  
4.0 |
| Veritas Operations Manager Thin Provisioning Reclamation Add-on       | 3.1.101.0  
3.1.201.0  
4.0 |
| Veritas Storage Foundation Add-on for Storage Provisioning           | 4.0 |
| Veritas Storage Foundation Add-on for Veritas Volume Replicator Bandwidth reporting | 3.1.101.0 |

**Note:** When you upgrade your existing Management Server installation to Veritas Operations Manager 4.0, the status of the Add-ons with the versions that are not supported in Veritas Operations Manager 4.0 is displayed as **Depricated** in the **Deployment Management** view. You must download and deploy the Add-ons with the versions that are supported in Veritas Operations Manager 4.0.

For the latest Veritas Operations Manager Add-ons, go to the following URL: [http://www.symantec.com/sfm_addons](http://www.symantec.com/sfm_addons)

See “**About deploying add-ons**” on page 73.

See “**About Veritas Operations Manager solutions**” on page 72.

**About deploying packages or patches**

You can download and install packages or patches for Veritas Operations Manager from the Symantec Web site. Packages or patches for Veritas Operations Manager are available either in tape archive (tar.gz) format or Storage Foundation archive (.sfa) format. To install the Veritas Operations Manager packages or patches, you must upload the packages or patches to the repository of management server.
About deploying hotfixes

You can install hotfixes for Veritas Operations Manager. You can upload one or more hotfixes to the repository, and then install them to the Management Server and the managed hosts.

**Note:** First you need to install the hotfix on the Management Server and then only Veritas Operations Manager lets you install that hotfix on managed hosts.

Viewing Veritas Operations Manager solutions in the repository

The Veritas Operations Manager solutions provide extended functionality to the users. In the **Deployment Management** view, you can view the solutions that are already uploaded to the Veritas Operations Manager repository. When a solution is uploaded, it is in the Not Installed state. To use the solution, you need to install it on hosts, server, or both (whichever is applicable for the solution). Once the solution is installed, you can enable or disable it.

The **Deployment Management** displays the following details:

- **Solution:** The name of the solution.
- **Type:** The type of the solution - add-on, package, patch, or hotfix.
- **Scope:** The scope of the solution. It displays whether the solution is installed on a managed host, server, or on both.
- **Version:** The version of the installed solution.
- **Status:** The status of the solution. For example, installed, not installed, or enabled. You can view the hosts where you have installed the solution. For example, enabled (4 of 10) notifies that out of 10 hosts, the particular solution is installed on four hosts.
- **Platform:** The supported platform for the solution. For example, HP-UX, Linux, Windows and so on.
- **Description:** Additional information about the solution.
- **User Generated:** Indicates whether the user has created the add-on. Currently Veritas Operations Manager does not provide any option to the user to create new add-on. Therefore the value of **User Generated** field is set to No.

Refine your search based on the following filters:

- **Scope:** Select the scope of the solution that you want to search. For example, the solution that can be installed only on the Management Server/Central
Server (CS), only on the managed host (MH), and on both (CS+MH). Select Prebundled checkbox to search all the solutions that are pre-bundled with Veritas Operations Manager.

- **Type**: Select the solution type that you want to search. For example, add-on, package, patch, or hotfix.

- **Platform**: Select the platform. For example, to search the solutions that can be installed only on AIX, you need to select AIX checkbox. Veritas Operations Manager displays all the solutions that can be installed on AIX platform (irrespective of their scope and type).

### To view solutions in the repository

- In the Veritas Operations Manager console, select Settings > Deployment Management. In the Deployment Management view, you can view the available solutions.

See “Installing Veritas Operations Manager solution” on page 78.

See “Uninstalling a solution” on page 81.

See “Viewing the solution deployment summary and the hosts to install solution” on page 82.

See “Canceling the deployment request for a solution” on page 87.

See “Downloading the deployment log for a solution’s deployment request” on page 88.

---

## Uploading a solution to repository

After you have downloaded the solution for Veritas Operations Manager from Symantec Web site, you need to upload it. After you upload the solution, you need to install it, and then you can start using it.

### To upload a solution to repository

1. In the Veritas Operations Manager console, click Settings > Deployment Management.

2. In the Deployment Management view, do one of the following:
   - Click **Upload**.
   - Right-click in the table, and from the submenu select **Upload**.

3. In **Upload to Repository** panel, click **Browse** and select the solution that you want to upload.
4 Click **Upload** to upload the solution to the repository.

5 Click **Close**.

See “Installing Veritas Operations Manager solution” on page 78.

See “Removing a Veritas Operations Manager solution from repository” on page 82.

See “Viewing deployment request details for a solution” on page 87.

## Installing Veritas Operations Manager solution

Use this page to view the instructions to select solution from the list of all solutions that are uploaded to the repository, and then install it on managed hosts or Management Server. In the **Deployment Management** view, under **Scope** column, you can view which solution can be installed on managed host (MH Only), Management Server/Central Server (CS Only), or on both (MH+CS).

**Note:** If the solution is a hotfix, first you need to install it on the Management Server/Central Server, and then on the managed hosts.

---

### To install a solution

1 In the Veritas Operations Manager console, select **Settings > Deployment Management**.

2 In the **Deployment Management** view, select the solution that you want to install and then do one of the following:

   - Click **Install**.
   - Right-click the solution and then select **Install**.

3 You see options in the **Install Solution** panel depending on whether you have selected solution to install only on managed hosts or Management Server.

   - For Management Server: No selection is required from the user. The solution is installed directly on the Management Server. If the solution is already installed on the Management Server, this operation overwrites the earlier installation. You need to restart the Web server on the Management Server after the successful installation of solution.

   - For managed hosts: Select the required option (**Hosts** or **Platforms**).

4 Click **Install**.

5 In the **Result** panel, click **OK**

See “Install solution options” on page 79.
See “Downloading the deployment log for a solution's deployment request” on page 88.

See “Installing solutions on specific managed hosts” on page 84.

Install solution options

The solutions can be installed on:

■ Management Server
■ Managed hosts
■ Both

If you select to install a solution (applicable only for managed hosts), you see Hosts and Platforms options in the wizard panel. If you select to install a solution (applicable only for Management Server), these options are not available. In that scenario, the application installs the solution on the Management Server, or overwrites the solution if it is already installed.

Use this panel to install the uploaded solutions on managed hosts or Management Server. For managed hosts, you can either select the hosts explicitly, or you can select the platform. When you select a specific platform, the solution is installed on all the managed hosts using that platform.

Table 4-2 Install solution options for managed hosts

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>Select to view the list all managed hosts where the solution is not installed.</td>
</tr>
<tr>
<td></td>
<td>If you select the <strong>Show all applicable hosts (Overwrites existing installation)</strong> option, you can see all the managed hosts where you can install the solution. It includes:</td>
</tr>
<tr>
<td></td>
<td>■ Managed hosts on which the solution is not installed currently.</td>
</tr>
<tr>
<td></td>
<td>■ Managed hosts where the solution is installed currently. In this scenario, Veritas Operations Manager overwrites the existing solution installation.</td>
</tr>
</tbody>
</table>
Table 4-2 Install solution options for managed hosts (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platforms</td>
<td>Select to install the solution on all managed hosts using the specific operating system. For example, if you select Windows in the list, the application installs the solution on all the hosts that use Windows operating system. This option is also useful to install the solution whenever a new managed host using the specific operating system is added to the Management Server. Select <strong>Force Install (Overwrites existing installation)</strong> option to overwrite existing solution installation on the managed hosts.</td>
</tr>
<tr>
<td>Install</td>
<td>Start the installation. After the installation, a deployment request is sent. The solution is installed asynchronously. You can check its status on the <strong>Deployment Summary</strong> page.</td>
</tr>
</tbody>
</table>

See “Installing Veritas Operations Manager solution” on page 78.

Upgrading managed hosts using Veritas Operations Manager console

Users can upgrade multiple managed hosts (that is upgrading VRTSsfmh package on these hosts) using Veritas Operations Manager console. This is an efficient method to upgrade VRTSsfmh package remotely on these managed hosts (instead of upgrading VRTSsfmh package on these hosts individually). This section explains how to upgrade VRTSsfmh package on managed hosts using Veritas Operations Manager console. To upgrade the managed hosts, ensure that VRTSsfmh package is already uploaded to the repository. In the same context, note that if any hot fix (for VRTSsfmh package) is installed on the managed hosts, you need not remove that hot fix before upgrading the VRTSsfmh package. You can directly proceed with upgrading the VRTSsfmh package.
To upgrade managed hosts using Veritas Operations Manager

1. In the Veritas Operations Manager console, click **Settings > Deployment Management**.

2. In the **Deployment Management** view, select the package (VRTSfmh package), and do one of the following:
   - Click **Install**.
   - Right-click the solution, and from the submenu select **Install**.

3. In the **Install Solution** panel, click **Hosts** option, and select the desired managed hosts. If you want to upgrade all managed hosts that use a specific platform, use the **Platforms** option.

4. Click **Install**.

5. Verify the managed host version in the console.
   
   See “Verifying the version of a Veritas Operations Manager managed host in the console” on page 24.

Uninstalling a solution

You can uninstall a solution from the Management Server and managed host. You can uninstall only add-on; package or patch cannot be uninstalled. After you uninstall an add-on, you cannot enable or disable it. If the uninstalled add-on is applicable to the Management Server, you need to restart the Web server on the Management Server after you uninstall the add-on successfully.

---

**Note:** You cannot uninstall pre-bundled add-ons.

To uninstall a solution

1. In the Veritas Operations Manager console, select **Settings > Deployment Management**.

2. In the **Deployment Management** view, select the add-on that you want to uninstall and do one of the following:
   - Click **Uninstall**.
   - Right-click the add-on and then select **Uninstall**.

3. In the **Uninstall solution from all hosts** panel, click **OK**.

   See “Enabling the solution on specific managed hosts” on page 84.
   
   See “Disabling the solution on specific managed host” on page 85.
Removing a Veritas Operations Manager solution from repository

You can remove Veritas Operations Manager solution from the solution repository. You need to uninstall the solution (add-on, hotfix, or distribution) before you remove it. That is, the add-on must be in Not Installed state before you remove it. You cannot remove the solutions, which are pre-bundled with Veritas Operations Manager. You can remove one solution at a time.

Note: If the solution is a hotfix, first you need to remove it from all managed hosts, and then from the Management Server/Central Server.

To remove an add-on

1 In the Veritas Operations Manager console, select Settings > Deployment Management.
2 In the Deployment Management view, select the add-on that you want to remove and do one of the following:
   ■ Click Remove.
   ■ Right-click the add-on and then select Remove.
3 In the Remove solution from repository panel, click OK.

Viewing the solution deployment summary and the hosts to install solution

Use this page to view the deployment summary of the solution and the hosts where you can install the solution.

In the Deployment Summary view, you can review the following information:

■ Version: The version of the selected solution.
■ Type: The type of the solution. For example, package and add-on.
■ Description: Additional information about the solution.
The pie chart displays the number of hosts where the solution is in Installed, Enabled, Disabled, or Not Installed state. In the bar chart, you can view the host details and their states along with the information on their operating systems. When you click a specific portion of these charts, the host details in **Hosts** table changes dynamically.

Select the appropriate option under the **Hosts** table to install, uninstall, enable, and disable solution for the selected host. For packages and patches, only **Install** option is available. For hotfix, **Install** and **Uninstall** options are available. For add-ons, **Install**, **Uninstall**, **Enable**, and **Disable** options are available to you.

Review the following host properties in the **Hosts** table:

- **Name**: Name of the managed host.
- **State**: Current state of the managed host. For example, Faulted, At Risk, Healthy and so on.
- **Status**: Solution status on the host. For example, Installed, Not Installed and so on.
- **Architecture**: Managed host's architecture. For example, SPARC, x86, x86_64 and so on.
- **Platform**: Managed host's platform. For example, Windows, HP-UX, Solaris and so on.
- **Family**: Managed host's operating system family. For example, Solaris, Windows Server NT, Red Hat Enterprise Linux and so on.
- **OS Version**: Version of the operating system.
- **MH Version**: Version of the managed host.

**To view the hosts to install solution**

1. In the Veritas Operations Manager console, select **Settings > Deployment Management**.
2. In the **Deployment Management** view, click the desired add-on or package.
3. In the **Deployment Summary** view, under **Hosts** tab, you can view the host details.

See “Installing solutions on specific managed hosts” on page 84.

See “Uninstalling solutions from specific managed hosts” on page 84.

See “Enabling the solution on specific managed hosts” on page 84.

See “Disabling the solution on specific managed host” on page 85.
Installing solutions on specific managed hosts

Use this option to install solution on the selected managed hosts of Veritas Operations Manager. If the solution is already installed on the selected host, the application overwrites the existing installation, and reinstall the solution. It is referred to as a force installation.

To install solution on specific managed hosts

1. In the Veritas Operations Manager console, click Settings > Deployment Management.
2. In the Deployment Management view, click the desired solution that you want to install on the managed hosts.
3. In the Deployment Summary view, under the Hosts table, you can view all the hosts where you can install the solution.
4. Select one or more hosts and click Install.
5. In the Install Solution panel click OK.

See “Uninstalling solutions from specific managed hosts” on page 84.

Uninstalling solutions from specific managed hosts

Use this option to uninstall the solution from one or more selected managed hosts of Veritas Operations Manager. This option is available only for add-on and hotfix. You can uninstall the solution irrespective of its state (enabled or disabled).

To uninstall solution from specific managed hosts

1. In the Veritas Operations Manager console, click Settings > Deployment Management.
2. In the Deployment Management view, click the desired solution that you want to uninstall from one or more managed hosts.
3. In the Deployment Summary view, under the Hosts table, select the host.
4. Click Uninstall.
5. In the Uninstall Solution panel click OK.

See “Installing solutions on specific managed hosts” on page 84.

Enabling the solution on specific managed hosts

Use this option to enable solution on one or more managed hosts of Veritas Operations Manager. This option is available only for add-on.
To enable solution on specific managed hosts

1. In the Veritas Operations Manager console, click Settings > Deployment Management.
2. In the Deployment Management view, click the desired solution that you want to enable on one or more managed hosts.
3. In the Deployment Summary view, in Hosts table, select the hosts where you want to enable the selected solution.
4. Click Enable.
5. In the Enable Solution wizard panel, and click OK.

See “Disabling the solution on specific managed host” on page 85.

Enable solutions on specific managed hosts options

You can use Enable Solution panel to enable solution, which is in the disabled state on managed hosts of Veritas Operations Manager. If the solution is already in enabled state, and if you try to enable it, Veritas Operations Manager overwrites the existing configuration (using Force option) on that managed host, and then again enable the solution. The enable operation is applicable only when the solution is already installed on the managed host.

See “Enabling the solution on specific managed hosts” on page 84.

Disabling the solution on specific managed host

Use this option to disable solution on one or more managed hosts of Veritas Operations Manager.

To disable solution on specific managed host

1. In the Veritas Operations Manager console, click Settings > Deployment Management.
2. In the Deployment Management view, click the desired solution that you want to disable on one or more managed hosts.
3. In the Deployment Summary view, in the Hosts table, select the hosts on which you want to disable the selected solution.
4. Click Disable.
5. In the Disable Solution wizard panel, and click OK.

See “Enabling the solution on specific managed hosts” on page 84.
Disable solutions on specific managed hosts options

You can use the **Disable Solution** wizard panel to disable the solution, which is in the enabled state on one or more managed hosts of Veritas Operations Manager. If the solution is already in disabled state, and if you try to disable it, Veritas Operations Manager overwrites the existing configuration (using Force option) on that managed host, and then again disable the solution.

See “Disabling the solution on specific managed host” on page 85.

Viewing the deployment requests for a solution

The **Deployment Requests** view lets you overview the details of deployment requests for a solution. You can view the following details:

- **Request Time**: Time and date when the request for the solution deployment was raised.
- **Operation**: The operation that was performed as a result of the request. For example, install and uninstall.
- **Type**: Deployment Request Type. For example Deploy by host and Deploy by platform.
- **Status**: Status of the deployment operation. For example Active and Canceled.
- **Result**: Result of the deployment. For example Finished, In-Progress and so on.
- **Hosts Succeeded**: The number of hosts where the solution deployment was successful.
- **Hosts Failed**: The number of hosts where the solution deployment failed.
- **Hosts In Progress**: The number of hosts where the solution deployment is in progress.
- **Total Hosts**: Total number of hosts.

Refine your search based on the following filters:

- **Status**: The present status of solution deployment request. For example, whether the request is still active or it is canceled.
- **Result**: The result of the deployment request. For example, whether it is in progress or finished.
- **Deployment Type**: The type of the deployment request. For example, by host or by platform.
To view the deployment requests for a solution

1. In the Veritas Operations Manager console, select Settings > Deployment Management.
2. In the Deployment Repository view, click the desired add-on or package.
3. In the Deployment Summary view, click the Requests tab. You can view all the requests that are related to the selected add-on or package.

See “Viewing deployment request details for a solution” on page 87.

Viewing deployment request details for a solution

Use this page to view the details of deployment requests for a specific add-on in Veritas Operations Manager. It displays the hosts where the add-on is installed or scheduled to install. Along with it, you can view the add-on operation status. For example, install success, uninstall success, and install scheduled.

To view deployment request details

1. In the Veritas Operations Manager console, select Settings > Deployment Management
2. In the Deployment Management view, click the desired add-on or package.
3. In the Deployment Summary view, click the Requests tab.
4. In the Deployment Requests view, select the request, and under Result column, click its status - Finished or In Progress.

See “Downloading the deployment log for a solution’s deployment request” on page 88.

See “Canceling the deployment request for a solution” on page 87.

Canceling the deployment request for a solution

Once you have started a solution deployment and if you want to cancel the request; you can do so using the Cancel Request option. However, you need to cancel the deployment request when it is in Progress state. Veritas Operations Manager does not let you cancel the deployment request if the deployment request is completed.

Note: You cannot cancel a deployment request that is of Deploy By Host type.
To cancel the deployment request for a solution

1. In the Veritas Operations Manager console, select **Settings > Deployment Management**.
2. In the **Deployment Management** view, click the desired add-on or package.
3. In the **Deployment Summary** view, click the **Requests** tab.
4. In **Deployment Requests** view, select the check box for the solution deployment request you want to cancel, and then do one of the following:
   - Click **Cancel Request**.
   - Right-click the desired deployment request and from the submenu select **Cancel Request**.
     The **Cancel Deployment Request** wizard panel displays the status message of the deployment operation.
5. In the **Cancel Deployment Request** wizard panel, click **OK**.

See “**Downloading the deployment log for a solution's deployment request**” on page 88.

See “**Enabling the solution on specific managed hosts**” on page 84.

See “**Disabling the solution on specific managed host**” on page 85.

See “**Removing a Veritas Operations Manager solution from repository**” on page 82.

### Downloading the deployment log for a solution's deployment request

For a selected solution, you can download the deployment log for its deployment requests. The deployment log file is a compressed file (tar.gz). You must have administrative privileges to download the deployment log.

**To download the deployment log for a solution's deployment request**

1. In the Veritas Operations Manager console, select **Settings > Deployment Management**.
2. In the **Deployment Management** view, click the desired add-on or package.
3. In the **Deployment Summary** view, click the **Requests** tab.
4. In the **Deployment Requests** view, select the deployment request for which you want to download its log, and then do one of the following:
   - Click **Download Deployment Log**.
Right-click the desired deployment request and from the submenu select **Download Deployment Log**.

5. Save the compressed file.

See “Canceling the deployment request for a solution” on page 87.

See “Viewing deployment request details for a solution” on page 87.
Deploying Veritas Operations Manager solutions

**Downloading the deployment log for a solution's deployment request**
Managing databases in Veritas Operations Manager

This chapter includes the following topics:

- Performing the database discovery for secure databases

Performing the database discovery for secure databases

Veritas Operations Manager discovers both the non-secure and the secure databases. Veritas Operations Manager does not require any configurations to discover the non-secure databases. For the secure databases, Veritas Operations Manager can discover the basic-level information without any authentication. To discover the secure databases using Veritas Operations Manager, you must authenticate the databases with the correct credentials. Veritas Operations Manager supports discovering the SQL, DB2, Sybase, and Oracle databases.

When you perform discovery of the Oracle databases, ensure that you have right permission to the following system tables:

- ALL_ARGUMENTS
- ALL_CATALOG
- ALL_COL_COMMENTS
- ALL_CONSTRAINTS
- ALLCONS_COLUMNS
- ALL_DB_LINKS
- ALL_ERRORS
- ALL_TAB_COMMENTS
- ALL_TRIGGER_COLS
- ALL_TRIGGER_COLS
- ALL_CONSTRAINTS
- ALL_CONS_COLUMNS
- ALL_ERRORS
- ALL_UPDATABLE_COLUMNS
- DBA_TS_QUOTAS
- DBA_USERS
- DBA_VIEWS
- DICTIONARY
- DICT_COLUMNS
To perform database discovery for a secure database

1. Select Manage > Databases.

2. If Veritas Operations Manager discovers any secure database instances, then you can view the following text at the top of the database list:

   There are Number of secure databases secure database instances that require credentials to perform full discovery. Click here to provide credentials.

   Click the link Click Here.

3. In the Select database instances panel, select the secure database that you want to authenticate, and click Next.

   See “Select database instances options” on page 93.

4. In the Provide Credentials panel, enter the required information, and click Next.

   See “Provide credentials options” on page 93.

5. In the Database Instance Credentials Summary panel, review the authentication information. Click Next.

   See “Database Instance Credentials Summary” on page 93.

6. In the Result panel, verify that the database instances have been authenticated successfully.
Select database instances options

Use this wizard panel to specify the secure databases that you want to authenticate. Select the check boxes to choose the database instances that you want to authenticate.

**Note:** You can choose multiple database instances if the credentials for the database instances are the same.

See “Performing the database discovery for secure databases” on page 91.

Provide credentials options

Use this wizard panel to specify the credentials to authenticate the database.

**Note:** These two options are available only for the SQL Server database instances. For discovering the database instances other than the SQL Server, Veritas Operations Manager uses only the domain authentication method, which prompts you to enter the user name and password for the domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/SQL Authentication</td>
<td>Choose this option to authenticate the database using the domain or SQL server credentials. Enter the user name and the password for the SQL server or the domain.</td>
</tr>
<tr>
<td>Operating System Authentication</td>
<td>Choose this option to authenticate the database using the administrator credentials for the operating system.</td>
</tr>
</tbody>
</table>

See “Performing the database discovery for secure databases” on page 91.

Database Instance Credentials Summary

Use this wizard panel to verify the authentication and the credential details. See “Performing the database discovery for secure databases” on page 91.
Managing databases in Veritas Operations Manager

Performing the database discovery for secure databases
Managing clusters in Veritas Operations Manager

This chapter includes the following topics:

- Viewing the fire drill schedules
- Modifying a fire drill schedule

Viewing the fire drill schedules

In Veritas Operations Manager, you can view the schedules that you have created for the high availability and the disaster recovery fire drills. This page also contains the list of fire drill schedules that failed.

Using the fire drill page, you can edit, enable, disable, or delete a fire drill schedule. This page displays the following information for a fire drill schedule:

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the fire drill schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The description for the fire drill that you entered when you configured it</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The schedule of the fire drill run</td>
</tr>
<tr>
<td>Start Date</td>
<td>The date when the fire drill was started</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the fire drill. Indicates whether the fire drill is enabled, disabled, or invalid.</td>
</tr>
</tbody>
</table>
The category of the fire drill. Indicates whether the schedule is for a high availability fire drill or a disaster recovery fire drill.

Details
Click the icon to view further details of the fire drill.

The fire drill schedules page displays the following information for a failed fire drill:

<table>
<thead>
<tr>
<th>Schedule Name</th>
<th>The name of the fire drill schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Category</td>
<td>The category of the fire drill. Indicates whether the schedule is for a high availability fire drill or a disaster recovery fire drill.</td>
</tr>
<tr>
<td>User</td>
<td>The name of the fire drill schedule along with the user name of the user who created the schedule.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The date and time when the fire drill was started</td>
</tr>
<tr>
<td>End Time</td>
<td>The date and time when the fire drill was finished</td>
</tr>
<tr>
<td>Details</td>
<td>Click on the icon to view the details of the failed fire drill schedule</td>
</tr>
</tbody>
</table>

To view the fire drill schedules and details

1 In the Veritas Operations Manager console, select **Policies > Fire Drills**.

2 Click **Schedules**.

See “Modifying a fire drill schedule” on page 96.

**Modifying a fire drill schedule**

Using Veritas Operations Manager, you can edit the schedules that you have created for running a high availability (HA) or a disaster recovery (DR) fire drill. You can identify the HA and the DR fire drills from the **Category** column in this page.
To modify a fire drill schedule

1. In the Veritas Operations Manager console, select **Policies > Fire Drills**.
2. Click **Schedules**.
3. In the schedules list, select the required fire drill schedule. Click **Edit**.
4. In the **Select Service Group(s)** wizard panel, verify the selection of the service groups for which you want to run the fire drill are selected. Click **Next**.
5. In the **Schedule** wizard panel, modify the schedule to run the fire drill. Click **Next**.
6. In the **Summary** panel, verify the selections that you have made. Click **Finish**.
7. In the **Result** panel, verify that the fire drill has been modified successfully.
Modifying a fire drill schedule
Managing hosts in Veritas Operations Manager

This chapter includes the following topics:

- About managing the hosts from Management Server
- Viewing the details of the managed hosts associated with Management Server
- Configuring the managed hosts to Management Server using the Web Console
- Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script
- Refreshing the details of the managed host
- Removing the managed hosts from Management Server
- About monitoring usage and configuring the automatic growth for file systems
- Setting the threshold for monitoring file system usage
- Configuring the automatic growth of the file systems
- About using Veritas Operations Manager to manage the hosts with Symantec ApplicationHA
- Enabling application heartbeat for a service group
- Disabling application heartbeat for a service group
About managing the hosts from Management Server

The current version of Veritas Operations Manager lets you manage hosts from Management Server. To perform the management tasks on the hosts, you must have the Admin role.

The following table lists the differences between the current and the previous versions of Veritas Operations Manager:

<table>
<thead>
<tr>
<th>Current Veritas Operations Manager version</th>
<th>Previous Veritas Operations Manager versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DNS server must be able to resolve the host name of Management Server, but not the managed host.</td>
<td>The DNS server must be able to resolve the host names of both Management Server and the managed host.</td>
</tr>
<tr>
<td>You must log in to Management Server to perform the management tasks on the hosts. Make sure that you can ping the managed host from Management Server.</td>
<td>You must log in to each managed host to perform the management tasks.</td>
</tr>
</tbody>
</table>

You can use the current release of Veritas Operations Manager to perform the following host management tasks:

- List the details of all managed hosts, including their statuses.
- Configure a new managed host to Management Server.
- Refresh the information about managed hosts.
- Remove managed hosts from Management Server.

See “Viewing the details of the managed hosts associated with Management Server” on page 101.

See “Configuring the managed hosts to Management Server using the Web Console” on page 102.

See “Refreshing the details of the managed host” on page 107.

See “Removing the managed hosts from Management Server” on page 107.
**Viewing the details of the managed hosts associated with Management Server**

In the **Settings > Host Management** view, under **Managed Hosts**, you can view the managed hosts that Management Server currently manages. A table displays the following information for each managed host:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Name or IP address of the managed host.</td>
</tr>
<tr>
<td>Host State</td>
<td>The state of the managed host. Host State can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Healthy – Management Server can discover the managed host and the</td>
</tr>
<tr>
<td></td>
<td>information that the host contains.</td>
</tr>
<tr>
<td></td>
<td>- At Risk – The managed host contains faulted objects or it uses the demo</td>
</tr>
<tr>
<td></td>
<td>license of Storage Foundation products.</td>
</tr>
<tr>
<td></td>
<td>A host can also be in the At Risk state because of any of the following</td>
</tr>
<tr>
<td></td>
<td>reasons:</td>
</tr>
<tr>
<td></td>
<td>- External faults</td>
</tr>
<tr>
<td></td>
<td>- VCS conditions</td>
</tr>
<tr>
<td></td>
<td>- VVR conditions</td>
</tr>
<tr>
<td></td>
<td>- Degraded DMP state</td>
</tr>
<tr>
<td></td>
<td>- Faulted – The managed host does not report to Management Server. Either</td>
</tr>
<tr>
<td></td>
<td>the managed host is no longer associated with Management Server or</td>
</tr>
<tr>
<td></td>
<td>Management Server cannot reach the host.</td>
</tr>
<tr>
<td>Last Ping Time</td>
<td>The latest date and time when managed host pinged the Management Server.</td>
</tr>
<tr>
<td>Platform</td>
<td>The platform of the managed host.</td>
</tr>
<tr>
<td>OS Version</td>
<td>The version of the operating system of the managed host.</td>
</tr>
<tr>
<td>MH Version</td>
<td>The Veritas Operations Manager version on the managed host.</td>
</tr>
<tr>
<td>Configuration Type</td>
<td>The configuration type of the managed host.</td>
</tr>
</tbody>
</table>
Discovery State/Time

State of hosts being configured or the last time the discovery data was reported for configured hosts. The discovery state can be one of the following:

- Probing
- Discovering

To filter the managed hosts based on their names, you can use the free text filter at the top of the table.

To filter the list of managed hosts

1. Select Settings > Host Management.
2. Under Managed Hosts, in the filter field, do one of the following:
   - Enter text to filter the list of managed hosts. You can filter the list based on any column in the table except the Last Ping Time. As you type in the filter box, the list of managed host is filtered to only show the hosts that match your text.
   - Paste text you want to use to filter the list of managed hosts and click Filter host. This filters the list of managed hosts to only show the hosts that match your text.

To view the details of managed hosts

1. Select Settings > Host Management.
2. Under Managed Hosts, view the table that lists managed hosts and their details.

   To view the details of a managed host, click on its name in the table.

See “Configuring the managed hosts to Management Server using the Web Console” on page 102.

See “Refreshing the details of the managed host” on page 107.

See “Removing the managed hosts from Management Server” on page 107.

Configuring the managed hosts to Management Server using the Web Console

To configure a new managed host to Management Server, you can use Configure Host(s) option under Settings > Host Management of Veritas Operations Manager console.
**Note:** Veritas Operations Manager does not support adding a managed host to Management Server if the version of the managed host is later than the version of Management Server. However, Veritas Operations Manager does not display any error messages when you perform this task.

You can add multiple hosts to Management Server. After you click **Submit**, you can view the operations that are finished, and the operations that are in progress on the subsequent page of the **Configure Host(s)** wizard.

You can view the details of the new-added host in the **Managed Hosts** table.

Before you configure a managed host to Management Server, make sure that the managed host can communicate with Management Server.

**To configure a managed host to the Management Server**

1. In the Veritas Operations Manager console, navigate to **Settings > Host Management**.

2. Click on **Configure Host(s)**.

3. In the **Configure Host(s)** wizard panel, enter the host details and click **Next**.

   See “**Configure host options**” on page 103.

4. In the **Results** panel, verify that the host has been added successfully. Click **OK**.

   See “**About managing the hosts from Management Server**” on page 100.

   See “**Viewing the details of the managed hosts associated with Management Server**” on page 101.

   See “**Refreshing the details of the managed host**” on page 107.

**Configure host options**

Use this wizard panel to specify options for configuring a managed host to Management Server.

You can also use this wizard panel to configure multiple hosts at once by importing the information from a comma-separated (.csv) file from a specified location. The CSV file must include the “.csv” extension.

The following is an example of a CSV file that includes user names and passwords for each host:
Host, User, Password
host1, user1, password1
host2, user2, password2

Table 7-2 Configure host wizard panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Host name or IP address that you can use to reach the managed host from Management Server.</td>
</tr>
<tr>
<td>User name</td>
<td>User name with administrator rights.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to log on to the managed host.</td>
</tr>
<tr>
<td>Add entries</td>
<td>Lets you manually specify more than one host to add.</td>
</tr>
</tbody>
</table>

See “Configuring the managed hosts to Management Server using the Web Console” on page 102.

Adding managed hosts to Management Server using the Auto Configure (gendeploy.pl) script

You can add a managed host to the Management Server domain with minimal user interaction. The Auto Configure (gendeploy.pl) script available on the Management Server can be used to create a script that is run on the managed host to add the host to the domain. You can create the script either at the command prompt, or in the Veritas Operations Manager Management Server console.

You need to copy the script that is created using gendeploy.pl to all the managed hosts that you want to add to the domain. After you copy the script, you have to run it on each managed host. A managed host on which you run the script must have the VRTSsfm plugin installed on it.

**Note:** Adding many managed hosts to Management Server at the same time using the Auto Configure (gendeploy.pl) script can affect the performance of Management Server. It is recommended that you phase deployment of managed hosts so that no more than 50 managed hosts are being added at any given moment.

See the Veritas Operations Manager Installation Guide for information on installing Veritas Operations Manager host management.
To add a managed host to a UNIX-based Management Server using the Auto Configure (gendeploy.pl) script

1 Create the script to add a managed host using either the command prompt, or the console. Do one of the following:
   ■ Log on to the Veritas Operations Manager Management Server console as an Admin user. Select Settings > Host Management. In the Host Management view, click Auto Configure button. In the Auto Configure dialog, click Download. In the File Download dialog, click Save to save the script to the required location.
   ■ On the Management Server, log on as root.
     Run the following command:
     /opt/VRTSsfmh/bin/gendeploy.pl --out <filename> [--domain <domain name>]
     Where, filename is the name of the script that you specify. The domain name is the Management Server host name.

2 Copy the script to the managed host.

3 On the managed host, change the directory to the location where you copied the script.

4 Do one of the following:
   ■ On UNIX-based hosts, run the following command to make the script executable:
     chmod +x filename
     Where, filename is the name of the script.
     Run the script:
     ./filename
   ■ On Windows-based hosts, run the following command:
     "C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe" filename
     Where, filename is the name of the script.
     For the above script, the optional hostname parameter is the managed host as seen by the Veritas Operations Manager Management Server. The host is discovered by this name or IP address in Veritas Operations Manager.

5 In the console, verify that the managed host has been added to the Management Server domain.
To add a managed host to a Windows-based Management Server using the Auto configure (gendeploy.pl) script

1. Create the script to add a managed host using either the command prompt, or the console. Do one of the following:

   ■ Log on to the Veritas Operations Manager Management Server console as an Admin user. Select **Settings > Host Management.** In the **Host Management** view, click **Auto Configure** button. In the **Auto Configure** dialog, click **Download.** In the **File Download** dialog, click **Save** to save the script to the required location.

   ■ On Management Server, log on as a user with administrator privileges. To change the directory, run the following command at the command prompt:

   ```
   cd "C:\Program Files\Veritas\VRTSsfmh\bin"
   ```

   To create the script to add a managed host, run the following command:

   ```
   perl.exe gendeploy.pl --out <filename> [--domain <domain name>]
   ```

   Where, *filename* is the name of the script that you specify. The *domain name* is the Management Server host name.

2. Copy the script to the managed host.

3. On the managed host, change the directory to the location where you copied the script.

4. Do one of the following:

   ■ On UNIX-based hosts, run the following command to make the script executable:

   ```
   chmod +x filename
   ```

   Where, *filename* is the name of the script.

   Run the script:
   ```
   ./filename
   ```

   ■ On Windows-based hosts, run the following command:

   ```
   "C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe" filename
   ```

   Where, *filename* is the name of the script.

   For the above script, the optional hostname parameter is the managed host as seen by the Veritas Operations Manager Management Server. The host is discovered by this name or IP address in Veritas Operations Manager.

5. In the console, verify that the managed host has been added to the Management Server domain.
Refreshing the details of the managed host

To refresh the discovery of the agent families on a managed host, you can use the Refresh Host(s) option.

You can also perform this task under the Host view in the Manage > Hosts view.

Note: You can perform the Refresh Hosts task on one or more managed hosts at a time.

To refresh the details of a managed host

1. Do one of the following
   - Select Manage > Hosts.
   - Select Settings > Host Management.

2. In the table that lists the managed hosts, select the managed host that you want to refresh and do one of the following:
   - At the top of the table, click the Refresh Host(s) option.
   - Right-click the managed host and from the submenu select the Refresh Host(s) option.

3. In the wizard panel to confirm the refresh operation, click OK.

See “About managing the hosts from Management Server” on page 100.

See “Viewing the details of the managed hosts associated with Management Server” on page 101.

See “Configuring the managed hosts to Management Server using the Web Console” on page 102.

Removing the managed hosts from Management Server

If you want to dissociate the managed hosts from Management Server and remove the managed hosts from the database, you can use the Remove Host(s) option.

To remove the managed hosts from Management Server

1. Select Settings > Host Management.

2. In the table that lists the managed hosts, select the managed host that you want to remove and do one of the following:
At the top of the table, click the **Remove Host(s)** option.

Right-click the managed host and from the submenu select the **Remove Host(s)** option.

3. In the wizard panel to confirm the remove operation, click **OK**.

See “About managing the hosts from Management Server” on page 100.

See “Viewing the details of the managed hosts associated with Management Server” on page 101.

### About monitoring usage and configuring the automatic growth for file systems

In Veritas Operations Manager, the capacity and the usage of file systems are very important because it directly affects the performance of the applications that use these file systems. Therefore, the administrators need to constantly monitor the usage of the file systems in their environment and prevent any faults that may happen to it.

Veritas Operations Manager provides you options to set thresholds for monitoring the file system usage and plan preventive measures to avoid file system failures. The system notifies you with adequate alerts if the current usage exceeds threshold levels. This feature also provides the capability to increase the size of the file system at a predefined stage. These options include the following:

- Setting up threshold values for triggering alerts when the file system usage crosses a specific limit
- Specifying the amount of space that you want to increase on the file systems when the file system usage crosses a specified limit.

In Veritas, you can configure two types of thresholds to trigger alerts based on the file system usage. The High Usage Warning, which is the low threshold, triggers risk alert when the file system usage crosses the limit that you have specified. It lets you identify and address the space issues early. The High Usage Risk threshold, which is highest threshold, triggers the fault alert that needs the urgent attention from administrators.

The optimal performance of the file systems in your environment is directly related to the amount of free space in them. You can configure the file system to grow automatically by a specified value when the usage of the file system crosses high threshold, that is the High Usage Risk. When you choose this option, Veritas Operations Manager increases the size of the file system if enough space is available on the volume. If the volume does not have enough space for increasing the size of the file system, Veritas Operations Manager increases the size of the
volume, which automatically increases the size of the file system in an equivalent proportion. Veritas Operations Manager uses a system rule which executes the canned script for increasing the size of the file system. This rule is executed when the Management Server receives the fault alert that is triggered when the file system crosses the High Usage Risk threshold. You cannot edit or delete this system rule.

In a clustered file system environment where the file system has been mounted on multiple servers, the master node triggers the fault alert and resizes the file system when the file system crosses the High Usage Risk threshold.

Before doing this operation, you must ensure that you have enough space on the disk or the disk group to increase the size of the volume. If the disk or the disk group does not have enough space to increase the size of the volume, the system rule which executes the canned script for increasing the file system size fails and raises an alert.

The automatic growth operation is supported only for the VxFS File Systems, which are mounted on the VxVM volumes that are not configured under Veritas Volume Replicator. Also, the automatic growth operation is not supported for the VxFS File Systems that are mounted on the VxVM volume sets.

**Note:** For a fault, Veritas Operations Manager triggers the alert only once. If the file system usage is greater than the High Usage Risk threshold value after a successful automatic growth operation, you must reset the High Usage Risk threshold value to let Veritas Operations Manager trigger fault alerts when the file system crosses the High Usage Risk threshold at a later time. Veritas Operations Manager does not trigger further fault alerts until a fault is addressed by resetting the High Usage Risk threshold value.

See “Setting the threshold for monitoring file system usage” on page 109.

See “Configuring the automatic growth of the file systems” on page 112.

**Setting the threshold for monitoring file system usage**

In Veritas Operations Manager, you can monitor the usage of the file systems in your environment. To monitor the file system usage, you can set the High Usage Warning and the High Usage Risk thresholds. The High Usage Warning threshold triggers risk alert when the file system usage crosses the limit that you have specified. The High Usage Risk triggers the fault alert that needs your urgent attention. You can view these alerts in the **Alerts** page of Veritas Operations Manager.
To perform this operation, you must have the administrator or the operator privilege on the parent host of the file system.

In Veritas Operations Manager, you can do this operation from any locations where you can find a file system.

**To set the threshold for monitoring file system usage**

1. In the Veritas Operations Manager console, click **Manage > Hosts**.
2. In the page that lists the hosts, click on the required host.
3. In the Host details page, click **File Systems**.
4. Do one of the following:
   - Select the required file systems, and select **More > Monitor Capacity**.
   - Right-click on the required file system and select **Monitor Capacity**.
5. In the **Monitor Capacity** wizard panel, enter the information in the **High Usage Warn (%)** and in the **High Usage Risk (%)** fields. Click **Next**.

See “**Monitor Capacity panel options**” on page 110.

6. In the **Monitor Capacity Summary** wizard panel, review the information that you have entered. Click **Finish**.

See “**Monitor Capacity Summary panel options**” on page 111.

7. In the **Result** page, verify that you have successfully configured the threshold values for monitoring the file system usage.

See “**About monitoring usage and configuring the automatic growth for file systems**” on page 108.

**Monitor Capacity panel options**

Using this wizard panel, you can do the following operations:

- Setting the threshold values for monitoring the file system usage
- Specifying the amount of space that you want to increase on the file system

**Table 7-3 Monitor Capacity panel options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply to all systems</strong></td>
<td>Select this check box to apply the threshold and autogrow values to all the file systems in the list. If you select this option, the fields threshold and autogrow fields under this check box are activated.</td>
</tr>
</tbody>
</table>
### Table 7-3  Monitor Capacity panel options *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount Point</td>
<td>The location where the file system is mounted</td>
</tr>
<tr>
<td>Host</td>
<td>The host where the file system resides</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the file system</td>
</tr>
<tr>
<td>Size</td>
<td>The total size of the file system</td>
</tr>
<tr>
<td>% Used</td>
<td>The amount of the used space on the file system in percentage</td>
</tr>
<tr>
<td>High Usage Warn (%)</td>
<td>Specify the size of the file system to trigger a risk alert on the Management Server</td>
</tr>
<tr>
<td>High Usage Risk (%)</td>
<td>Specify the size of the file system to trigger a fault alert on the Management Server</td>
</tr>
<tr>
<td>Autogrow (%)</td>
<td>Specify the amount of space that you want to increase on the file system when the file system crosses the high usage risk threshold</td>
</tr>
</tbody>
</table>

See “Setting the threshold for monitoring file system usage” on page 109.
See “Configuring the automatic growth of the file systems” on page 112.

### Monitor Capacity Summary panel options

Use this wizard panel to verify the information that you have entered for setting the threshold for monitoring your file systems, and for increasing the file system size.

### Table 7-4  Monitor Capacity Summary panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount Point</td>
<td>The location where the file system is mounted</td>
</tr>
<tr>
<td>Host</td>
<td>The host where the file system resides</td>
</tr>
<tr>
<td>Size</td>
<td>The total size of the file system</td>
</tr>
<tr>
<td>High Usage Warn (%)</td>
<td>The size of the file system at which you want Veritas Operations Manager to trigger a risk alert</td>
</tr>
</tbody>
</table>
### Configuring the automatic growth of the file systems

You can use the file system usage monitoring functionality in Veritas Operations Manager to increase the size of the file systems when they cross the High Usage Risk threshold. When you choose this option, Veritas Operations Manager increases the size of the file system if enough space is available on the volume. If the volume does not have enough space for increasing the size of the file system, Veritas Operations Manager increases the size of the volume, which automatically increases the size of the file system in an equivalent proportion.

To perform this operation, you must have the administrator privilege on the parent host of the file system.

In Veritas Operations Manager, you can do this operation from any locations where you can find a file system.

**To configure the automatic growth of the file systems**

1. In the Veritas Operations Manager console, click **Manage > Hosts**.
2. In the page that lists the hosts, click on the required host.
3. In the Host details page, click **File Systems**.
4. Do one of the following:
   - Select the required file systems and select **More > Monitor Capacity**.
   - Right-click on the required file system and select **Monitor Capacity**.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Usage Risk (%)</strong></td>
<td>The size of the file system at which you want Veritas Operations Manager to trigger a fault alert.</td>
</tr>
<tr>
<td><strong>Autogrow (%)</strong></td>
<td>The amount of space that you want to increase on the file system when the file system usage crosses the high usage risk threshold.</td>
</tr>
<tr>
<td><strong>Estimated approximate autogrow size</strong></td>
<td>The estimated size of the file system after the automatic growth is completed.</td>
</tr>
</tbody>
</table>

See “Setting the threshold for monitoring file system usage” on page 109.
See “Configuring the automatic growth of the file systems” on page 112.
5 In the Monitor Capacity wizard panel, enter the information in the High Usage Risk (%) and the Auto Grow (%) fields. Click Next.

See “Monitor Capacity panel options” on page 110.

6 In the Monitor Capacity Summary wizard panel, review the information that you have entered. Click Finish.

See “Monitor Capacity Summary panel options” on page 111.

7 In the Result page, verify that you have successfully configured the threshold and the automatic growth for monitoring the file system.

See “About monitoring usage and configuring the automatic growth for file systems” on page 108.

About using Veritas Operations Manager to manage the hosts with Symantec ApplicationHA

Symantec ApplicationHA provides enhanced monitoring capabilities for the applications that run on the virtual machines that are hosted on VMware ESX Servers. ApplicationHA uses the high availability concepts of agents, resources, and service groups. However, it does not include the high availability cluster components such as the Global Atomic Broadcast (GAB) and Low Latency Transport (LLT). You can install ApplicationHA on the Linux and the Windows platforms.

ApplicationHA can communicate directly with VMware HA with a mechanism called "heartbeat". If an application fails and the agents cannot start the application, ApplicationHA invokes a trigger that requests VMware HA to restart the virtual machine.

Veritas Operations Manager provides enhanced monitoring and reporting capabilities for the virtual machines that have ApplicationHA configured. The capabilities of Veritas Operations Manager to manage and monitor the applications and generate various types of reports help you manage the applications inside your virtual machines in a deeper level. To use Veritas Operations Manager to manage the applications on the virtual machines where ApplicationHA is installed, you must add all these virtual machines as hosts to Veritas Operations Manager using the Veritas Operations Manager console. If ApplicationHA is installed on these virtual machines, Veritas Operations Manager identifies the virtual machines as hosts, and the applications inside them as service groups. This lets you perform various high availability operations on the applications inside the virtual machines using the Veritas Operations Manager console. However, the high availability and the disaster recovery features such as readiness, fire drills, and global configuration of clusters are not supported in Veritas Operations Manager for the applications that are managed by ApplicationHA.
Veritas Operations Manager uses a service group that is created by ApplicationHA as the heartbeat agent for each virtual machine. You can identify this service group by the name "VCSAppMonHBSG". You must not perform any operations on this service group.

After you add the virtual machines as hosts to Veritas Operations Manager, Veritas Operations Manager uses a consistent monitoring mechanism to monitor the applications that run on these virtual servers. This mechanism lets the administrators of the VMware vCenter Servers identify the problems with the configured applications, and take necessary steps to rectify it. In some cases, you may not want the VMware vCenter Servers to act upon the faults on certain systems or service groups. In such cases, Veritas Operations Manager gives you options to disable the fault reporting function. You can enable the fault reporting anytime after you disable it.

Veritas Operations Manager console displays the hosts and the service groups individually when it displays the information pertaining to the objects of ApplicationHA.

Note: ApplicationHA includes the VRTSsfmh package version 3.0.358 that has been shipped with Veritas Operations Manager version 3.0 RU1. You must upgrade the VRTSsfmh package to version 3.1 or later to use Veritas Operations Manager to manage the virtual machines that have ApplicationHA installed. For more information on how to upgrade the VRTSsfmh package, refer the Veritas Operations Manager 4.0 Installation Guide.

Enabling application heartbeat for a service group

Symantec ApplicationHA sends consistent messages to the VMware vCenter Server. These messages, normally called as "heartbeats" lets the VMware vCenter Server know about the health of a service group. In certain situations, you may not want to propagate the faults on a service group to the VMware vCenter Server because the actions that the server performs to resolve the fault (mostly starting or stopping of the virtual machine) can result in the downtime of the entire virtual machine. In such situations, you can disable the heartbeats and then enable it using the Veritas Operations Manager console.

When you enable the heartbeat on a service group, the heartbeat is enabled for all other service groups in the same host.

To perform this operation, you must have the administrator privileges on the service groups where you are enabling the application heartbeat.
To enable the application heartbeat service groups

1 In the Veritas Operations Manager console, do one of the following to locate the service groups:
   - To locate the service groups in the list of all service groups, select Manage > Service Groups.
   - To locate the service groups in a host, select Manage > Hosts and click Service Groups.

2 Do one of the following:
   - Select the check boxes to select the service groups to enable the application heartbeat. Click More above the service groups list and select Enable Application Heartbeat.
   - To enable the application heartbeat for a single service group, right-click on the row of the service group to display the shortcut menu. In case of multiple service groups, first select the check box for each service group, and then, right-click on any of the rows to display the shortcut menu. From the shortcut menu, select Enable Application Heartbeat.

3 In the Enable Application Heartbeat page, click OK.

4 In the Result page, verify that the operation was successful. Click OK.

See “About using Veritas Operations Manager to manage the hosts with Symantec ApplicationHA” on page 113.

Disabling application heartbeat for a service group

Symantec ApplicationHA sends consistent messages to the VMware vCenter Server. These messages, normally called as "heartbeats" lets the VMware vCenter Server know about the health of a service group. In certain situations, you may not want to propagate the faults on a service group to the VMware vCenter Server because the actions that the server performs to resolve the fault (mostly starting or stopping of the virtual machine) can result in the downtime of the entire virtual machine. In such situations, you can disable the heartbeats using the Veritas Operations Manager console.

When you disable the heartbeat on a service group, the heartbeat is disabled for all other service groups in the same host.

To perform this operation, you must have the administrator privileges on the service groups where you are disabling the application heartbeat.
To disable the application heartbeat service groups

1  In the Veritas Operations Manager console, do one of the following to locate the service groups:
   ■ To locate the service groups in a host, select Manage > Hosts and click Service Groups.
   ■ To locate the service groups in the list of all service groups, select Manage > Service Groups.

2  Do one of the following:
   ■ Select the check boxes to select the service groups to disable the application heartbeat. Click More above the service groups list and select Disable Application Heartbeat.
   ■ To disable the application heartbeat for a single service group, right-click on the row of the service group to display the shortcut menu. In case of multiple service groups, first select the check box for each service group, and then, right-click on any of the rows to display the shortcut menu. From the shortcut menu, select Disable Application Heartbeat.

3  In the Disable Application Heartbeat page, click OK.

4  In the Result page, verify that the operation was successful. Click OK.

See “About using Veritas Operations Manager to manage the hosts with Symantec ApplicationHA” on page 113.
Discovering the server virtualization environment using Veritas Operations Manager

This chapter includes the following topics:

- About the virtualization technologies supported by Veritas Operations Manager
- About Control Hosts in Veritas Operations Manager
- About discovering the VMware Infrastructure using Veritas Operations Manager
- Viewing the Virtualization Management view
- Configuring the VMware discovery in Veritas Operations Manager
- Editing a VMware discovery configuration in Veritas Operations Manager
- Refreshing a VMware discovery configuration in Veritas Operations Manager
- Removing a VMware discovery configuration in Veritas Operations Manager
- About discovering Solaris zones in Veritas Operations Manager
- About discovering Logical domains in Veritas Operations Manager
- About the reports related to virtualization in Veritas Operations Manager
- Viewing the summary of virtualization in Veritas Operations Manager
About the virtualization technologies supported by Veritas Operations Manager

Datacenters adopt virtualization technology to effectively use the IT-infrastructure and substantially reduce the capital and operational expenditures. If you have adopted virtualization technology in your datacenter, Veritas Operations Manager provides you an efficient way of discovering and managing your virtual storage and infrastructure assets.

In your datacenter, Veritas Operations Manager helps you view the following relationships:

■ Applications in your datacenter that Veritas Operations Manager manages and the virtual hosts on which they are running.

■ Physical storage in your datacenter that is exported to the virtual machines.

Veritas Operations Manager supports the following virtualization technologies:

■ VMware virtualization technology

■ Solaris Zones

■ Solaris Logical Domains (LDom).

In the VMware virtualization technology that Veritas Operations Manager supports, a designated Control Host discovers the VirtualCenter servers in the datacenter. This discovery displays the ESX servers that the VirtualCenter server manages and the virtual machines that are configured on the ESX servers. Veritas Operations Manager can also discover the ESX servers that VirtualCenter servers do not manage.

In the Solaris zones virtualization technology that Veritas Operations Manager supports, the Zone agentlet that is present in the \texttt{VRTSsfmh} package, which is installed on a Solaris managed host discovers the Global Zones that are configured on the host. This discovery displays the non-global zones that are configured on the Global Zone.

In the Solaris LDom virtualization technology that Veritas Operations Manager supports, the LDom agentlet that is present in the \texttt{VRTSsfmh} package, which is installed on a Solaris managed host discovers the LDom Server that is configured on the host. This discovery displays the LDoms that are configured on the LDom Server.
Also, you generate the following reports that displays the details of the virtual environment that Veritas Operations Manager discovers:

- All Virtual Machines
- All Virtualization Servers
- All Datastores.

See “About discovering the VMware Infrastructure using Veritas Operations Manager” on page 121.

See “About discovering Solaris zones in Veritas Operations Manager” on page 134.

See “About discovering Logical domains in Veritas Operations Manager” on page 139.

See “About the reports related to virtualization in Veritas Operations Manager” on page 143.

About Control Hosts in Veritas Operations Manager

Veritas Operations Manager uses Control Hosts as a discovery mechanism. In Veritas Operations Manager, the Control Hosts discovers the following:

- Deep array information on the enclosures that Storage Insight Add-on supports. To configure this Control Host on a managed host, you need to install the binaries from the vendor on the managed host.

- Information on VMware Virtualization Infrastructure. To configure this Control Host on a managed host, you need to install the Control Host Add-on on the managed host.

Storage Insight Add-on supports the following enclosures:

- HITACHI
- IBM XIV
- EMC Symmetrix
- EMC CLARiiON
- NetApp

On the vendor enclosures that Storage Insight Add-on supports, the Control Hosts discover the following additional information on the enclosures:

- Logical devices
- Physical devices
- Thin pools
Host associations

Replications

To discover the deep array information on the enclosures using Storage Insight Add-on, you can configure the Control Host on any managed host. Ideally, you must configure two managed hosts as Control Hosts. You can designate the first managed host as Primary Control Host and the second managed host as Secondary Control Host. The Secondary Control Host acts as a backup if the Primary Control Host goes down.

To configure a managed host as a Control Host for discovering the deep array information on the enclosures from any of the vendors that Storage Insight Add-on supports, you must install the binaries provided by the vendor on the managed host. For example, to configure the Control Hosts for discovering the deep array information on the EMC CLARiiON enclosure, you must install the NaviSphere CLI binaries with version 6.29 or later on the managed hosts that you want to designate as the Primary and the Secondary Control Hosts.

In Veritas Operations Manager, you can configure Veritas Operations Manager Management Server or a managed host that reports to Management Server as Control Host for discovering the information on the VMware virtualization infrastructure. For this configuration, you must install the Control Host Add-on on the hosts that you want to designate as Control Host. In Veritas Operations Manager, you must download the Control Host Add-on from the Symantec Web site, upload to the Deployment Management Repository, and install it on the relevant hosts.

In your datacenter, Control Hosts help Management Server in discovering the following information on VMware virtualization infrastructure:

- VMware VirtualCenter servers that are configured in your datacenter.
- VMware ESX servers that Virtual Centers manage.
- VMware Virtual machines that are configured on the VMware ESX servers.

In Veritas Operations Manager, you can install the Control Host Add-on on the managed hosts with the following platforms:

- Solaris 10 (SPARC)
- Linux (64-bit)
- Windows Server 2003/2008 (64-bit)

For information on managing an Add-on in Veritas Operations Manager, see Veritas Operations Manager Administrator's Guide

Ensure that the Control Hosts can ping the VirtualCenter servers or the ESX servers from which they can discover the information on VMware Infrastructure.
The Control Host discovers the VMware Infrastructure from the hosts other than Management Server. After the discovery of VMware Infrastructure, the Control Host reports the discovered data to Management Server. Management Server coalesces the data that it receives from the Control Host and populates the relevant views.

You can designate a managed host that reports to Management Server as Control Host to address the following situations:

- To discover the VirtualCenter server that is behind a firewall and you do not want to install Management Server inside the firewall.
- To except Management Server from the discovery of VMware infrastructure to reduce the load on Management Server.

See “About discovering the VMware Infrastructure using Veritas Operations Manager” on page 121.

See “How Veritas Operations Manager discovers VirtualCenter and ESX servers” on page 124.

See “Information that Veritas Operations Manager discovers on the VMware Infrastructure components” on page 125.

See “Configuring the VMware discovery in Veritas Operations Manager” on page 127.

### About discovering the VMware Infrastructure using Veritas Operations Manager

In Veritas Operations Manager, a managed host that is designated as a Control Host can discover the VMware Infrastructure.

The managed host on which you have installed the Control Host Add-on discovers the information on the following VMware infrastructure components in your datacenter:

- VirtualCenter servers, which manage one or more ESX servers.
- ESX servers on which the individual virtual machines are configured.

A VirtualCenter or an ESX server does not need to be a managed host to let the Control Host to discover them.

Ensure that the Control Hosts can ping the VirtualCenter servers or the ESX servers from which they can discover the information on VMware Infrastructure. Ideally, a Control Host and a VirtualCenter server or an ESX server from which the Control Host wants to discover the information on VMware Infrastructure must be on the same subnet.
The Control Host Add-on that you install on the designated Control Hosts contains the VMware Infrastructure SDK (VI SDK), which provides a standard interface for the VMware servers and the Control Hosts to access the VMware Infrastructure. A Control Host reports the information on the VMware Infrastructure that it discovers to Management Server. Management Server coalesces the data that it receives from the Control Host and populates the relevant views.

**Note:** If you have installed Storage Insight Add-on 4.0, Veritas Operations Manager can correlate the storage that is visible to the ESX servers with the storage enclosures that Storage Insight Add-on supports.

In Veritas Operations Manager, you must configure the storage enclosure discovery using Storage Insight Add-on before you configure the discovery of the VirtualCenter and the ESX servers.

If you configure the storage enclosure discovery after you configure the discovery of the VirtualCenter and the ESX servers, then the storage enclosure details become visible to the ESX servers from the next discovery cycle.

A designated Control Host in Veritas Operations Manager discovers the following versions of VirtualCenter and ESX servers:

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Version Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualCenter Servers</td>
<td>From version 2.5 to version 4.1</td>
</tr>
<tr>
<td>ESX Servers</td>
<td>From version 3.5 to version 4.1</td>
</tr>
</tbody>
</table>

See “About the virtualization technologies supported by Veritas Operations Manager” on page 118.

See “About Control Hosts in Veritas Operations Manager” on page 119.

See “Requirements for discovering VirtualCenter and ESX servers using Veritas Operations Manager” on page 123.

See “How Veritas Operations Manager discovers VirtualCenter and ESX servers” on page 124.

See “Information that Veritas Operations Manager discovers on the VMware Infrastructure components” on page 125.

See “About the datastores in Veritas Operations Manager” on page 125.

See “Limitations of the discovery of VirtualCenter and ESX servers using Veritas Operations Manager” on page 126.

See “Configuring the VMware discovery in Veritas Operations Manager” on page 127.
The following are the requirements for discovering VMware Infrastructure using Veritas Operations Manager:

- Install the VRTSsfmh package on the hosts on which you want to install the Control Host Add-on.

- Ensure that the Control Hosts can ping the VirtualCenter servers or the ESX servers from which they can discover the information on VMware Infrastructure. Ideally, a Control Host and a VirtualCenter server or an ESX server from which the Control Host wants to discover the information on VMware Infrastructure must be on the same subnet.

- Ensure that you have appropriate privileges to log on to the VirtualCenter server or the ESX server.

- Ensure that you have the Browse Datastore privileges on the VirtualCenter or the ESX server that you want Veritas Operations Manager to discover.

- Ensure that the VirtualCenter servers that the Control Host wants to discover are with versions 2.5 and later.

- Ensure that the ESX servers that the Control Host wants to discover are with versions 3.5 and later.

See “About discovering the VMware Infrastructure using Veritas Operations Manager” on page 121.

See “How Veritas Operations Manager discovers VirtualCenter and ESX servers” on page 124.

See “Information that Veritas Operations Manager discovers on the VMware Infrastructure components” on page 125.

See “Limitations of the discovery of VirtualCenter and ESX servers using Veritas Operations Manager” on page 126.
How Veritas Operations Manager discovers VirtualCenter and ESX servers

Veritas Operations Manager uses designated Control Hosts to discover the information on the virtual machines. You must install the Control Host Add-on on the managed hosts that you want to designate as Control Hosts. Control Host uses the VMware Infrastructure SDK (VI SDK) to access the VirtualCenter and the ESX servers.

Ensure that the Control Hosts can ping the VirtualCenter servers or the ESX servers from which they can discover the information on VMware Infrastructure. Ideally, a Control Host and a VirtualCenter server or an ESX server from which the Control Host wants to discover the information on VMware Infrastructure must be on the same subnet.

When you configure the virtualization discovery in Veritas Operations Manager, you must ensure that you have appropriate privileges to access the VirtualCenter or the ESX servers. Also, you must ensure that you have Browse Datastore privileges on the VirtualCenter or the ESX servers from which you want to discover the VMware Infrastructure information.

The VirtualCenter or the ESX servers contains a Web server, which is an Apache Tomcat server. The web services that are hosted on the Web server communicate with the VMware Infrastructure. After you configure a virtualization discovery, the Control Host uses VI SDK to communicate with the web services that are hosted on the Web server. For this communication, the Control Host uses the HTTPS protocol.

The URL for the VMware SDK web services is as follows:

https://host name of the VirtualCenter or the ESX servers/sdk

After the discovery of VMware Infrastructure, the Control Host reports the discovered data to Management Server. Management Server coalesces the data that it receives from the Control Host and populates the relevant views.

See “About discovering the VMware Infrastructure using Veritas Operations Manager” on page 121.

See “Requirements for discovering VirtualCenter and ESX servers using Veritas Operations Manager” on page 123.

See “Information that Veritas Operations Manager discovers on the VMware Infrastructure components” on page 125.

See “About the datastores in Veritas Operations Manager” on page 125.

See “Limitations of the discovery of VirtualCenter and ESX servers using Veritas Operations Manager” on page 126.
Information that Veritas Operations Manager discovers on the VMware Infrastructure components

Discovery of the VMware Infrastructure components provides the following information:

- Host name and IP address of the VMware Infrastructure components that Veritas Operations Manager discovers.
- Operating system handles of the VMware Infrastructure components that Veritas Operations Manager discovers.
- Correlation of operating system handles to the virtual disks that are associated with the virtual machines configured on the ESX servers.

See “About discovering the VMware Infrastructure using Veritas Operations Manager” on page 121.

See “Requirements for discovering VirtualCenter and ESX servers using Veritas Operations Manager” on page 123.

See “How Veritas Operations Manager discovers VirtualCenter and ESX servers” on page 124.

See “About the datastores in Veritas Operations Manager” on page 125.

See “Limitations of the discovery of VirtualCenter and ESX servers using Veritas Operations Manager” on page 126.

See “Viewing the summary of virtualization in Veritas Operations Manager” on page 143.

See “Viewing virtualization servers in Veritas Operations Manager” on page 144.

See “Viewing the virtual machines in Veritas Operations Manager” on page 146.

About the datastores in Veritas Operations Manager

A datastore is a collection of physical storage that is created based on the disks and LUNs that are attached to an ESX server. The storage is assigned to VMware virtual machines from the datastore. Veritas Operations Manager lets you view the storage mapping between the datastore and the virtual machines.
A datastore is a storage location for virtual machine files. This storage location can be a VMFS volume, a directory on Network Attached Storage, or a local file system path.

Also, VMware can assign storage to the virtual machines directly from the physical disks that are available with the ESX servers. This storage assignment is known as Raw Disk Assignment.

See “About discovering the VMware Infrastructure using Veritas Operations Manager” on page 121.

Limitations of the discovery of VirtualCenter and ESX servers using Veritas Operations Manager

The following limitations apply to the discovery of VMware Infrastructure using Veritas Operations Manager:

- Veritas Operations Manager cannot discover the VirtualCenter servers that are lower than the version 2.5.
- Veritas Operations Manager cannot discover the ESX servers that are lower than the version 3.5.

See “About discovering the VMware Infrastructure using Veritas Operations Manager” on page 121.

See “Requirements for discovering VirtualCenter and ESX servers using Veritas Operations Manager” on page 123.

See “Information that Veritas Operations Manager discovers on the VMware Infrastructure components” on page 125.

Viewing the Virtualization Management view

In Veritas Operations Manager, the Virtualization Management view displays the information on the VMware Infrastructure that Veritas Operations Manager discovers. In this view, a tree-table structure displays the information on the VirtualCenter servers and the ESX servers that Veritas Operations Manager discovers.

In the Virtualization Management view, you can perform the following tasks:

- Configure VMware VirtualCenter server and ESX servers discovery.
- Edit the VirtualCenter server and ESX server discovery that you have already configured.
- Refresh a VirtualCenter server to view the periodic discovery of ESX servers that it manages.
Remove a VirtualCenter server or an ESX server that Veritas Operations Manager discovers.

In the Virtualization Management view, you can view the following details of a VirtualCenter server or an ESX server:

- Host name of the VirtualCenter server or the ESX server that Veritas Operations Manager discovers. If Veritas Operations Manager discovers a VirtualCenter server, you can click the + sign on the left side of the VirtualCenter server name to view the ESX servers that the VirtualCenter manages.

- Type of the host that Veritas Operations Manager discovers. This field specifies whether the host is a VirtualCenter server or an ESX server.

- Host name of the Control Host, which is used to discover the VirtualCenter server or the ESX server.

- Name that you have specified for the VMware discovery configuration.

- State of the configuration. If the VirtualCenter discovery is successful, this field displays the configuration state as Successful. For an ESX server, this field displays the date and time at which the discovery occurred. Also, this field displays the status of the latest discovery cycle for an ESX server.

To view the Virtualization Management view

- In the Veritas Operations Manager console, select Settings > Virtualization Management.

See “Configuring the VMware discovery in Veritas Operations Manager” on page 127.

See “Editing a VMware discovery configuration in Veritas Operations Manager” on page 130.

See “Refreshing a VMware discovery configuration in Veritas Operations Manager” on page 132.

See “Removing a VMware discovery configuration in Veritas Operations Manager” on page 133.

Configuring the VMware discovery in Veritas Operations Manager

In Veritas Operations Manager, you must configure the VMware discovery to let a Control Host discover the VirtualCenter and ESX servers.

The discovery of a VirtualCenter server provides the following information:

- Information on VirtualCenter servers
Information on the ESX servers that the VirtualCenter server manages

Information on the virtual machines that are configured on the ESX servers.

In Veritas Operations Manager, you can use the Virtualization Configuration wizard panel to configure the VMware discovery.

After you configure VMware discovery in Veritas Operations Manager, you can view the VirtualCenter servers, which Veritas Operations Manager discovers, in a table in the Virtualization Management view. All ESX servers that each VirtualCenter server manages are displayed as children under the VirtualCenter server.

To configure VMware discovery in Veritas Operations Manager

1. In the Veritas Operations Manager console, select Settings > Virtualization Management.

2. In the Virtualization Management view, click Add Configuration.

3. In the Virtualization Configuration wizard panel, enter the details and click Next.
   
   See “Virtualization Configuration panel options” on page 128.

4. In the Virtualization Configuration progress details wizard panel, view the progress of the configuration and click OK.
   
   See “Virtualization Configuration progress details panel” on page 130.

See “Editing a VMware discovery configuration in Veritas Operations Manager” on page 130.

See “Refreshing a VMware discovery configuration in Veritas Operations Manager” on page 132.

See “Removing a VMware discovery configuration in Veritas Operations Manager” on page 133.

See “Viewing the Virtualization Management view” on page 126.

Virtualization Configuration panel options

Use this wizard panel to configure VMware discovery in Veritas Operations Manager. You can configure the VMware discovery based on a VirtualCenter server or an ESX server.
### Table 8-1 Virtualization Configuration panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Type</strong></td>
<td>Select the configuration type from the drop-down list. By default, this field displays the configuration type as VMware.</td>
</tr>
<tr>
<td><strong>VMware Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration Name</td>
<td>Enter a name for the VMware discovery configuration. You can reference the new VMware discovery configuration with the name that you specify in this field.</td>
</tr>
<tr>
<td>Control Host</td>
<td>Select the name of the control host from the drop-down list. Veritas Operations Manager uses the Control Host that you specify in this field to discover the VMware environment that VirtualCenter and ESX servers manage. You must ensure that you can ping the VirtualCenter or the ESX server from the Control Host. Typically, the Control Host and the VirtualCenter or the ESX servers should belong to the same subnet.</td>
</tr>
<tr>
<td>Server</td>
<td>Fully-qualified name of the VirtualCenter or ESX server that you want the Control Host to discover. Alternatively, you can also specify the IP address of the server.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user name that you can use to log on to the VirtualCenter or ESX servers that you want the Control Host to discover. You can use a read-only user account if it has the Datastore Browse permissions on the VirtualCenter or the ESX servers.  <strong>Note:</strong> Ensure that you have appropriate privileges to log in to the VirtualCenter or the ESX servers.</td>
</tr>
</tbody>
</table>
Table 8-1 Virtualization Configuration panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter the password that you can use along with the user name to log on to the VirtualCenter or ESX servers that you want the Control Host to discover.</td>
</tr>
</tbody>
</table>

See “Configuring the VMware discovery in Veritas Operations Manager” on page 127.

Virtualization Configuration progress details panel

Use this wizard panel to view the progress of the virtualization discovery configuration. This panel displays the start and the successful completion of the virtualization discovery.

See “Configuring the VMware discovery in Veritas Operations Manager” on page 127.

Editing a VMware discovery configuration in Veritas Operations Manager

In Veritas Operations Manager, you can edit the VMware discovery that you have already configured.

You can edit a VMware discovery configuration to modify the following information:

- Name of the configuration.
- Name of the VirtualCenter server that you have specified when you configured the VMware discovery.
- Credentials to log on to the VirtualCenter server.

To edit a VMware discovery configuration in Veritas Operations Manager

1. In the Veritas Operations Manager console, select Settings > Virtualization Management.
2. In the Virtualization Management view, in the table that displays the details of the VMware discovery configurations, select the configuration that you want to edit.
3. At the top of the table, which displays the VMware discovery configurations, click Edit Configuration.
4 In the Virtualization Configuration wizard panel, modify the required information and click Next.

See “Virtualization Configuration panel options (Edit)” on page 131.

5 In the Virtualization Configuration progress details wizard panel, view the progress of the configuration and click OK.

See “Virtualization Configuration progress details panel (Edit)” on page 132.

See “Configuring the VMware discovery in Veritas Operations Manager” on page 127.

See “Refreshing a VMware discovery configuration in Veritas Operations Manager” on page 132.

See “Removing a VMware discovery configuration in Veritas Operations Manager” on page 133.

See “Viewing the Virtualization Management view” on page 126.

Virtualization Configuration panel options (Edit)

Use this wizard panel to edit the VMware discovery that you have configured in Veritas Operations Manager.

Table 8-2  Virtualization Configuration panel options for editing the VMware discovery configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Type</td>
<td>Displays the configuration type as VMware.</td>
</tr>
<tr>
<td>VMware Configuration</td>
<td></td>
</tr>
<tr>
<td>Configuration Name</td>
<td>Displays the name that is provided to the VMware discovery configuration.</td>
</tr>
<tr>
<td></td>
<td>You can modify the name of the configuration in this field.</td>
</tr>
<tr>
<td>Control Host</td>
<td>Displays the name of the control host that is specified for discovering the VirtualCenter servers and ESX servers that Veritas Operations Manager manages.</td>
</tr>
<tr>
<td>VMware VCenter Server</td>
<td>Displays the name of the VirtualCenter server that you have specified when you configured the VMware discovery. You can modify the name of the server in this field.</td>
</tr>
</tbody>
</table>
Table 8-2 Virtualization Configuration panel options for editing the VMware discovery configuration (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Displays the user name that you can use to log on to the VirtualCenter or ESX servers that you have specified. You can modify the user name in this field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that you have appropriate privileges to log in to the VirtualCenter or the ESX servers.</td>
</tr>
<tr>
<td>Password</td>
<td>Displays the password that you can use along with the user name to log on to the VirtualCenter or ESX servers that you have specified. You can modify the password in this field.</td>
</tr>
</tbody>
</table>

See “Editing a VMware discovery configuration in Veritas Operations Manager” on page 130.

**Virtualization Configuration progress details panel (Edit)**

Use this wizard panel to view the progress of the virtualization discovery configuration update. This panel displays the start and the successful update of the virtualization discovery configuration.

See “Editing a VMware discovery configuration in Veritas Operations Manager” on page 130.

**Refreshing a VMware discovery configuration in Veritas Operations Manager**

In Veritas Operations Manager, you can refresh the VirtualCenter server that Veritas Operations Manager has already discovered.

**To refresh a VMware discovery configuration in Veritas Operations Manager**

1. In the Veritas Operations Manager console, select **Settings > Virtualization Management**.

2. In the **Virtualization Management** view, in the table that displays the details of the VMware discovery configurations, select the configuration that you want to refresh.
3  At the top of the table, which displays the VMware discovery configurations, click **Refresh Configuration**.

4  In the **Refresh Virtualization Configuration** wizard panel, view the progress of the refresh task. After the refresh of the selected VMware discovery configuration is completed, the **Refresh Virtualization Configuration** panel displays the message that the refresh is successfully completed.

5  Click **OK**.

See “**Configuring the VMware discovery in Veritas Operations Manager**” on page 127.

See “**Editing a VMware discovery configuration in Veritas Operations Manager**” on page 130.

See “**Removing a VMware discovery configuration in Veritas Operations Manager**” on page 133.

See “**Viewing the Virtualization Management view**” on page 126.

---

**Removing a VMware discovery configuration in Veritas Operations Manager**

In Veritas Operations Manager, you can remove a VMware discovery configuration.

**To remove a VMware discovery configuration in Veritas Operations Manager**

1. In the Veritas Operations Manager console, select **Settings > Virtualization Management**.

2. In the **Virtualization Management** view, in the table that displays the details of the VMware discovery configurations, select the configuration that you want to remove.

3. At the top of the table, which displays the VMware discovery configurations, click **Remove Configuration**.

4. In the **Remove Virtualization Configuration** wizard panel, click **Remove**.

5. In the panel that confirms the confirmation, click **OK**.

See “**Configuring the VMware discovery in Veritas Operations Manager**” on page 127.

See “**Editing a VMware discovery configuration in Veritas Operations Manager**” on page 130.

See “**Refreshing a VMware discovery configuration in Veritas Operations Manager**” on page 132.
About discovering Solaris zones in Veritas Operations Manager

Solaris zones and Solaris Resource Manager are the components of Solaris Container environment. A Solaris zone is a virtualized operating system environment that is created within a Solaris 10 operating system instance. You can run your applications on the virtualized operating system services that you have created using Solaris zones.

Two types of Solaris zones are Global Zones and non-Global Zones. In a single instance of Solaris operating system, a Global Zone administers multiple non-Global Zones. Each non-Global Zone is isolated from other non-Global Zones. The IP address, host name, security context, applications, and the processes that run on each non-Global Zone are completely isolated from the other non-Global Zones.

Veritas Operations Manager discovers the zones that are created on a Solaris 10 host that it manages. The Zone Agentlet that is installed along with the VRTSafm package on a Solaris 10 host lets the Veritas Operations Manager Management Server to discover the Global Zones and the non-Global Zones on the host.

Through the discovery of Solaris zones, Veritas Operations Manager discovers the following information:

- The non-Global Zones that are associated with a Global Zone.
- The storage that is exported from the Global Zone to non-Global Zones.
- Databases that run in non-Global Zones.

**Note:** Veritas Operations Manager discovers the Oracle databases on a non-Global Zone only if the non-Global Zone is in the Running state.

**Note:** Veritas Operations Manager does not support the discovery of the applications other than the Oracle databases on non-Global Zones.

See “Requirements for discovering Solaris zones in Veritas Operations Manager” on page 135.

See “How Veritas Operations Manager discovers Solaris zones” on page 136.

See “Information that Veritas Operations Manager discovers on Solaris zones” on page 137.
Requirements for discovering Solaris zones in Veritas Operations Manager

The following are the requirements for discovering Solaris zones in Veritas Operations Manager:

- Install the `VRTSsfmh` package on one or more hosts that contains Global Zones. This helps Veritas Operations Manager discover non-global-zones that are configured on the Global Zones.
- Ensure that the managed hosts with the Solaris 10 operating system contain non-Global Zones.
- Ensure that the managed hosts with the Solaris 10 operating system do not contain any LDoms.
- Enable the `zlogin` utility if you have already disabled it on the non-Global Zones.
  See “Requirements for the `zlogin` utility on non-Global Zones” on page 135.
- Ensure that the non-Global Zones can access the devices that are exported from the Global Zone.
  See “Requirements for devices exported to non-Global Zones” on page 136.
- Ensure that the file systems that are exported from the Global Zone to the non-Global Zones are mounted in the non-Global Zones.
  See “Requirements for file systems exported to non-Global Zones” on page 136.

See “About discovering Solaris zones in Veritas Operations Manager” on page 134.
See “How Veritas Operations Manager discovers Solaris zones” on page 136.
See “Information that Veritas Operations Manager discovers on Solaris zones” on page 137.
See “Limitations of the discovery of Solaris zones in Veritas Operations Manager” on page 138.

Requirements for the `zlogin` utility on non-Global Zones

Veritas Operations Manager uses the `zlogin` utility to discover non-Global Zones. By default, the `zlogin` utility is enabled on non-Global Zones. If you have disabled the `zlogin` utility on non-Global Zones, you need to enable it.
For example, you might have disabled the `zlogin` utility by adding the following line to the `/etc/pam.conf` configuration file on a non-Global Zone:

```
zlogin auth required pam_deny.so.1
```

See “Requirements for discovering Solaris zones in Veritas Operations Manager” on page 135.

**Requirements for devices exported to non-Global Zones**

Veritas Operations Manager can discover the devices that are exported from the Global Zone to non-Global Zones. However, if the storage is not accessible to the non-Global Zone, Veritas Operations Manager cannot discover that storage as exported from the Global Zone. For example, the storage may not be accessible to the non-Global Zone because the non-Global Zone was not yet restarted. Ensure that the non-Global Zones can access the devices that are exported from the Global Zone.

See “Requirements for discovering Solaris zones in Veritas Operations Manager” on page 135.

**Requirements for file systems exported to non-Global Zones**

Veritas Operations Manager can discover the file systems that are exported from the Global Zone to non-Global Zones. However, if a file system is not mounted in a non-Global Zone, Veritas Operations Manager does not discover that file system as exported from the Global Zone. Ensure that the file systems that are exported from the Global Zone to the non-Global Zones are mounted in the non-Global Zones.

See “Requirements for discovering Solaris zones in Veritas Operations Manager” on page 135.

**How Veritas Operations Manager discovers Solaris zones**

In Veritas Operations Manager, the zone agentlet that is part of the `VRTSsfmh` package facilitates the discovery of Solaris zones on a Solaris 10 managed host. Through the zone agentlet, Veritas Operations Manager discovers the Global Zone and the associated non-Global Zones.

**Note:** Discovery of zones is performed only in the Global Zones.

Veritas Operations Manager uses the following Solaris utilities to discover global and non-Global Zones:
Table 8-3  Solaris utilities to discover global and non-Global Zones

<table>
<thead>
<tr>
<th>Utility</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>zoneadm</td>
<td>Lists the non-Global Zones that are configured on the Global Zone on the Solaris 10 managed host</td>
</tr>
<tr>
<td>zonecfg</td>
<td>Displays the details of each non-global configurations</td>
</tr>
<tr>
<td>zlogin</td>
<td>Logs on to a non-Global Zone from a Global Zone.</td>
</tr>
</tbody>
</table>

See “About discovering Solaris zones in Veritas Operations Manager” on page 134.
See “Requirements for discovering Solaris zones in Veritas Operations Manager” on page 135.
See “Information that Veritas Operations Manager discovers on Solaris zones” on page 137.
See “Limitations of the discovery of Solaris zones in Veritas Operations Manager” on page 138.

Information that Veritas Operations Manager discovers on Solaris zones

Discovery of Solaris zones provides the following information:

Table 8-4  Solaris zones information that Veritas Operations Manager discovers

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Global Zones , which are configured on Global Zones</td>
<td>Veritas Operations Manager discovers the following:</td>
</tr>
<tr>
<td></td>
<td>■ The devices that are exported from the Global Zone to the non-Global Zones.</td>
</tr>
<tr>
<td></td>
<td>■ The file systems that are mounted in the non-Global Zones.</td>
</tr>
<tr>
<td>Storage that is exported from the Global Zone to the non-Global Zones</td>
<td>Veritas Operations Manager discovers the following:</td>
</tr>
<tr>
<td></td>
<td>■ Full operating system handles (not slices)</td>
</tr>
<tr>
<td></td>
<td>■ Veritas Volume Manager volumes</td>
</tr>
<tr>
<td></td>
<td>■ ZFS volumes</td>
</tr>
</tbody>
</table>
Table 8-4  Solaris zones information that Veritas Operations Manager discovers (continued)

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle databases inside non-Global Zones</td>
<td>Veritas Operations Manager discovers the following:</td>
</tr>
<tr>
<td>■ Oracle databases</td>
<td>■ Oracle databases</td>
</tr>
<tr>
<td>■ Oracle RAC databases</td>
<td>■ Oracle RAC databases</td>
</tr>
<tr>
<td>■ Oracle database on solaris9 branded</td>
<td>■ Oracle database on solaris9 branded zone.</td>
</tr>
<tr>
<td>zone.</td>
<td>■ Oracle database on Solaris native branded zone.</td>
</tr>
<tr>
<td>■ Oracle database on Solaris native</td>
<td>Note: Veritas Operations Manager does not support the discovery of secure Oracle databases on the non-Global Zones. A secure Oracle database has a password-set on 'sysdba' account to secure them.</td>
</tr>
<tr>
<td>branded zone.</td>
<td></td>
</tr>
</tbody>
</table>

See “About discovering Solaris zones in Veritas Operations Manager” on page 134.

See “Requirements for discovering Solaris zones in Veritas Operations Manager” on page 135.

See “How Veritas Operations Manager discovers Solaris zones” on page 136.

See “Limitations of the discovery of Solaris zones in Veritas Operations Manager” on page 138.

Limitations of the discovery of Solaris zones in Veritas Operations Manager

The following limitations apply to the discovery of Solaris zones in Veritas Operations Manager:

■ Veritas Operations Manager does not support the discovery of Solaris zones on Solaris managed hosts where both the zones and the LDoms are configured.

■ Veritas Operations Manager does not recommend the installation of the VRTSafmh package in non-Global Zones.

Note: Conversely, you can install Veritas Operations Manager Management Server in a non-Global Zone and add the corresponding Global Zone as a managed host to Management Server.
Veritas Operations Manager does not discover the devices that are exported to non-Global Zones if the `zlogin` utility is not allowed on them.

Veritas Operations Manager discovers only the native and the Solaris-branded zones.

See “About discovering Solaris zones in Veritas Operations Manager” on page 134.

See “Requirements for discovering Solaris zones in Veritas Operations Manager” on page 135.

See “How Veritas Operations Manager discovers Solaris zones” on page 136.

See “Information that Veritas Operations Manager discovers on Solaris zones” on page 137.

### About discovering Logical domains in Veritas Operations Manager

Logical Domains (LDoms) is the paravirtualization technology from Oracle Sun. An LDom provides a separate virtualized operating system environment and a virtualized CPU that are created within a Solaris operating system instance. Each LDom uses an independent kernel. Each LDom contains a dedicated, virtualized operating system, and a virtualized CPU. You can start, stop, and restart the operating system that run inside an LDom. Each LDom functions as a full virtual machine with a subset of hardware resources that you can configure as required. You can run your applications on the LDoms.

The physical server in your datacenter on which the LDoms are created is known as LDom Server. Individual Guest LDoms that are created on an LDom Server can have several different roles, which are based on the context and usage of the LDoms.

The following are the four major types of roles of the LDoms:

<table>
<thead>
<tr>
<th>Table 8-5 LDom roles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LDom role</strong></td>
</tr>
<tr>
<td>Control domain</td>
</tr>
</tbody>
</table>
Table 8-5  LDom roles (continued)

<table>
<thead>
<tr>
<th>LDom role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service domain</td>
<td>Provides the services to other LDom that are created on the LDom Server. For example, the Service domain provides a virtual network switch or a virtual disk service.</td>
</tr>
<tr>
<td>I/O domain</td>
<td>Accesses the input or output devices directly. For example, the I/O domain can access a network device.</td>
</tr>
<tr>
<td>Guest domain</td>
<td>Uses the services from the Service and the I/O domains. The Control domain manages the Guest domains.</td>
</tr>
</tbody>
</table>

The LDom Agentlet that is installed along with the VRTSsfmh package on a Solaris host lets the Veritas Operations Manager Management Server to discover the LDom Server and Guest LDom that are configured on the LDom server.

See “About the virtualization technologies supported by Veritas Operations Manager” on page 118.

See “Requirements for discovering Solaris Logical domains using Veritas Operations Manager” on page 140.

See “How Veritas Operations Manager discovers Solaris Logical domains” on page 141.

See “Information on Logical domains that Veritas Operations Manager discovers” on page 142.

See “Limitations of the discovery of Logical domains in Veritas Operations Manager” on page 142.

Requirements for discovering Solaris Logical domains using Veritas Operations Manager

The following are the requirements for discovering Solaris LDom using Veritas Operations Manager:

- Install the VRTSsfmh package on one or more hosts with the Solaris operating system on which you want Veritas Operations Manager to discover Solaris LDom.
- Ensure that the managed hosts with the Solaris operating system contain LDom.
See “About discovering Logical domains in Veritas Operations Manager” on page 139.

See “How Veritas Operations Manager discovers Solaris Logical domains” on page 141.

See “Information on Logical domains that Veritas Operations Manager discovers” on page 142.

See “Limitations of the discovery of Logical domains in Veritas Operations Manager” on page 142.

How Veritas Operations Manager discovers Solaris Logical domains

In Veritas Operations Manager, the LDom agentlet that is part of the VRTSsfmh package facilitates the discovery of LDoms on a Solaris managed host. Through the LDom agentlet, Veritas Operations Manager discovers the LDom Server and the associated Guest LDoms.

Veritas Operations Manager uses the ldm command to discover the details of Solaris Logical domains.

The following are the major options that Veritas Operations Manager uses with the ldm command to discover the details of Solaris Logical domains:

<table>
<thead>
<tr>
<th>ldm command and option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldm list</td>
<td>Lists all the LDoms that are configured on the LDom Server and their details.</td>
</tr>
<tr>
<td>ldm devices</td>
<td>Discovers the information on the CPU and memory of the LDoms that Veritas Operations Manager discovers.</td>
</tr>
</tbody>
</table>

See “About discovering Logical domains in Veritas Operations Manager” on page 139.

See “Requirements for discovering Solaris Logical domains using Veritas Operations Manager” on page 140.

See “Information on Logical domains that Veritas Operations Manager discovers” on page 142.

See “Limitations of the discovery of Logical domains in Veritas Operations Manager” on page 142.
Information on Logical domains that Veritas Operations Manager discovers

Discovery of Solaris LDoms provides the following information:

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest LDoms that are configured on LDom Servers</td>
<td>Veritas Operations Manager discovers the following:</td>
</tr>
<tr>
<td></td>
<td>■ Total number of Virtual CPUs.</td>
</tr>
<tr>
<td></td>
<td>■ Number of Virtual CPUs by core.</td>
</tr>
<tr>
<td></td>
<td>■ Number of Virtual CPUs that are assigned to each LDom.</td>
</tr>
<tr>
<td></td>
<td>■ Total system memory.</td>
</tr>
<tr>
<td></td>
<td>■ Available system memory.</td>
</tr>
<tr>
<td></td>
<td>■ Memory, which is assigned to each LDom.</td>
</tr>
</tbody>
</table>

See “About discovering Logical domains in Veritas Operations Manager” on page 139.

See “Requirements for discovering Solaris Logical domains using Veritas Operations Manager” on page 140.

See “How Veritas Operations Manager discovers Solaris Logical domains” on page 141.

See “Limitations of the discovery of Logical domains in Veritas Operations Manager” on page 142.

Limitations of the discovery of Logical domains in Veritas Operations Manager

The following limitations apply to the discovery of Solaris LDoms in Veritas Operations Manager:

■ Veritas Operations Manager does not discover the Solaris LDoms that are in the inactive state.

■ Veritas Operations Manager does not perform the discovery of Solaris LDoms along with the discovery of Solaris zones

See “About discovering Logical domains in Veritas Operations Manager” on page 139.
About the reports related to virtualization in Veritas Operations Manager

In Veritas Operations Manager, you can generate the following reports that display the details of the virtualization environment that Veritas Operations Manager discovers:

- **All Virtual Machines** report: Displays the details of all virtual machines in the datacenter that Veritas Operations Manager discovers.

- **All Virtualization Servers** report: Displays the details of all virtualization servers in the datacenter that Veritas Operations Manager discovers.

- **All Storage Pools** report: Displays the details of the storage pools in the datacenter that Veritas Operations Manager discovers.

See “About the virtualization technologies supported by Veritas Operations Manager” on page 118.

See “About discovering the VMware Infrastructure using Veritas Operations Manager” on page 121.

Viewing the summary of virtualization in Veritas Operations Manager

The **Virtualization** view displays the information on the virtual environment that Veritas Operations Manager discovers in its datacenter. The **Virtualization** view displays a bar chart that displays the number of virtual machines and virtualization servers. Distinct colors represent the virtual machines and virtualization servers of different virtualization technologies that Veritas Operations Manager supports. You can click the bar chart to view the details of virtual machines or virtualization servers.
At the bottom of the Virtualization view, you can view the Virtualization table that lists the details of the virtualization servers and virtual machines.

The Virtualization table lists the following details of the virtualization servers and the virtual machines of different virtualization technologies that Veritas Operations Manager supports:

- Total number of the virtualization servers and the virtual machines.
- Total number of the virtualization servers and the virtual machines that are faulted.
- Total number of the virtualization servers and the virtual machines that are at risk.
- Total number of the virtualization servers and the virtual machines that are healthy.

You can click the number that represents the virtual servers or the virtualization hosts under different categories to view its details.

To view the summary of virtualization in Veritas Operations Manager

- In the Veritas Operations Manager console, select Manage > Virtualization.

See “Viewing virtualization servers in Veritas Operations Manager” on page 144.
See “Viewing the virtual machines in Veritas Operations Manager” on page 146.

Viewing virtualization servers in Veritas Operations Manager

In the Virtualization Servers view, you can view the list of virtualization servers that Veritas Operations Manager manages. Virtualization servers hosts the virtual machines.

In the Virtualization Servers view, you can view the following types of virtualization servers:

- VMware ESX servers
- Logical Domain (LDom) Servers
- Global Zones

The Virtualization Servers view lists the following information on the virtualization servers that Veritas Operations Manager discovers:

- Name of the virtualization server.
- IP address of the virtualization server.
State of the virtualization server.
- Type of the virtualization server.
- Architecture of the operating system of the virtualization server.
- Family of the operating system of the virtualization server.
- Platform of the virtualization server.
- Version of the virtualization server's operating system.
- Version of Storage Foundation that is installed in the virtualization server.
- Version of the cluster that is associated with the virtualization server.
- Version of the VRTSsfmh package, which is installed on the virtualization server.
- Name of the cluster that is associated with the virtualization server.
- Configuration type of the virtualization server.
- Cluster technology that is associated with the virtualization server.
- Number of CPUs that are associated with the virtualization server.
- Current state of the virtualization server.
- Name of the virtualization server.
- Type of the virtualization server.

You can filter the Virtual Machines view based on the following:
- Status
- Platform
- Virtualization Type
- Configuration Type
- License

To view the virtualization servers in Veritas Operations Manager
- In the Veritas Operations Manager console, select Manage > Virtualization Servers.

See “Viewing the virtual machines in Veritas Operations Manager” on page 146.
See “Viewing the summary of virtualization in Veritas Operations Manager” on page 143.
Viewing the virtual machines in Veritas Operations Manager

In the Virtual Machines view, you can view the list of virtual machines that are configured on virtualization servers in Veritas Operations Manager.

In the Virtual Machines view, you can view the following types of virtual machines:

- VMware
- LDom
- Non-Global Zones

The Virtual Machines view displays the following information on the virtual machines:

- Name of the virtual machine.
- State of the virtual machine.
- Platform of the virtual machine.
- Version of the virtual machine's operating system.
- Version of Storage Foundation that is installed in the virtual machine.
- Memory that the virtual machine uses.
- Number of CPUs that are associated with the virtual machine.
- Name of the cluster that is associated with the virtual machine.
- Name of the virtualization server on which the virtual machine is configured.
- Configuration type of the virtual machine.
- Server type of the virtual machine.
- Version of the cluster that is associated with the virtual machine.
- Technology of the cluster that is associated with the virtual machine.
- Version of the VRTSsfmh package, which is installed on the virtual machine.
- Family of the operating system of the virtual machine.
- Architecture of the operating system of the virtual machine.
- Current state of the virtual machine.
- Type of the virtual machine.

You can filter the Virtual Machines view based on the following:

- Status
To view the virtual machines in Veritas Operations Manager

- In the Veritas Operations Manager console, select Manage > Virtual Machines.

See “Viewing virtualization servers in Veritas Operations Manager” on page 144.

See “Viewing the summary of virtualization in Veritas Operations Manager” on page 143.
Discovering the server virtualization environment using Veritas Operations Manager

Viewing the virtual machines in Veritas Operations Manager
Managing storage enclosures in Veritas Operations Manager

This chapter includes the following topics:

- Setting display name for a storage enclosure
- Setting display name for an array port

Setting display name for a storage enclosure

In Veritas Operations Manager, you can specify the display name for a storage enclosure.

To set display name for a storage enclosure

1. In the Veritas Operations Manager console, select Manage > Enclosures.
2. In the Enclosures view, do one of the following:
   - Select the check box for the enclosure for which you want to specify the display name and click Set Display Name.
   - Right-click the enclosure for which you want to specify the display name, and then click Set Display Name.
3 In the **Set displayable name for enclosure** panel, enter the names that you want to specify for the enclosure and the associated array ports, and click **OK**.

You can click **Set default** to revert to the default name.

See “**Set displayable name for enclosure options**” on page 150.

4 In the **Result** panel, verify that the operation was successful and click **OK**.

**Set displayable name for enclosure options**

Use this panel to specify the display name of the selected enclosure. You can also use this panel to specify the display names of the array ports that are associated with the enclosure that you have selected.

<table>
<thead>
<tr>
<th>Table 9-1</th>
<th>Set displayable name for enclosure options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Enclosure name</td>
<td>Enter the name that you want to specify for the enclosure.</td>
</tr>
<tr>
<td>Serial</td>
<td>The serial number of the enclosure.</td>
</tr>
<tr>
<td>Vendor</td>
<td>The vendor of the enclosure.</td>
</tr>
<tr>
<td>Product</td>
<td>The product name of the enclosure.</td>
</tr>
<tr>
<td>Array Ports</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the names that you want to specify for the array ports that are associated with the enclosure.</td>
</tr>
</tbody>
</table>

See “**Setting display name for a storage enclosure**” on page 149.

**Set displayable name for array port options**

Use this panel to specify the display name for the array port that you have selected.

<table>
<thead>
<tr>
<th>Table 9-2</th>
<th>Set displayable name for array port panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Arrayport name</td>
<td>Enter the name that you want to specify for the array port.</td>
</tr>
</tbody>
</table>

See “**Setting display name for a storage enclosure**” on page 149.
See “Setting display name for an array port” on page 151.

Setting display name for an array port

In Veritas Operations Manager, you can specify the display name for array ports.

To set display name for an array port

1. In the Veritas Operations Manager console, select Manage > Enclosures.

2. In the Enclosures view, click on the desired enclosure to view the enclosure details.

3. In the detailed view of the enclosure, click on the Array Ports tab.

4. In the Array Ports view, do one of the following:
   - Select the check box for the array port for which you want to specify the display name and click Set Display Name.
   - Right-click the array port for which you want to specify the display name, and then click Set Display Name.

5. In the Set displayable name for array port panel, enter the name that you want to specify for the selected array port and click OK.
   
   You can click Set default to revert to the default name.
   
   See “Set displayable name for array port options” on page 150.

6. In the Result panel, verify that the operation was successful and click OK.
Managing storage enclosures in Veritas Operations Manager

Setting display name for an array port
This chapter includes the following topics:

- Viewing the patches available to a host
- Viewing the details of a patch in the SORT Web site
- Setting up proxy server details to download patch information
- Downloading patch information in offline mode

**Viewing the patches available to a host**

Management Server of Veritas Operations Manager connects to Symantec Operations Readiness Tools (SORT) to let you review the information on the patches that Symantec releases. Also, you can download these patches to the desktop and deploy them in the datacenter.
In Veritas Operations Manager, under the Available Patches tab in the details view of a managed host, you can view the patches that are available for that host. Under the Available Patches tab, you can view the following details:

- Name of the product for which the patch is available.
- Type of the patch release.
- Size of the patch.
- Products for which you can apply the patch.
- The date and time at which the patch is released.
- Name of the release.
- Whether the patch is obsolete.

From the Product column, you can click the Details icon to view the details of the patch in the SORT Web site. From the Release name column, you can download a patch for the managed host on your desktop.

**To view the patches available for a host**

1. Select Manage > Hosts.
2. In the table that lists the hosts, click the name of the host to view its details.
3. In the details view of the host, click the Available Patches tab to view the patches that are available for the host.

**To download a patch to the desktop**

- Under the Available Patches tab, in the Patches table, in the Release Name column, click the download icon near to the name of the release to download the patch to the desktop.

See “Viewing the details of a patch in the SORT Web site” on page 154.
See “Setting up proxy server details to download patch information” on page 155.
See “Downloading patch information in offline mode” on page 156.

**Viewing the details of a patch in the SORT Web site**

In the Veritas Operations Manager console, you can click the Details icon to view the details of a patch in the Symantec Operations Readiness Tools (SORT) Web site.
To view the details of a patch in the SORT Web site

1. In the details view of a host, click the Available Patches tab to view the patches that are available for the host in the Patches table.

2. In the Products column of the table, click the Details icon near to the name of a product.

3. In the SORT Web site that is opened in a separate browser, review the details of the patch.

See “Viewing the patches available to a host” on page 153.

See “Downloading patch information in offline mode” on page 156.

See “Setting up proxy server details to download patch information” on page 155.

Setting up proxy server details to download patch information

To download information on the Storage Foundation and the Storage Foundation and High Availability patches from Symantec, Management Server of Veritas Operations Manager must be connected to Symantec Web site. Management Server of Veritas Operations Manager requires https connectivity with the vos.symantec.com server for downloading the information that is related to the Storage Foundation and the Storage Foundation and High Availability patches. The Management Server of Veritas Operations Manager uses the https://sort.symantec.com link to communicate with the web service for getting the patch information.

If you cannot connect Management Server of Veritas Operations Manager to the Symantec Web site directly, you can set up an alternate proxy server that can access Symantec Web site. Make sure that the proxy server has https connectivity with the sort.symantec.com server for tunneling the request. Management Server of Veritas Operations Manager must talk to the proxy server on the configured port.

Also, you can set up the download schedule for the patches. You must check the Enable Patch Information Download check box to activate the proxy server to connect to Symantec Web site.

To set up proxy server details to download patch information

1. Select Settings > Management Server.

2. In the Management Server Settings page, in the Patch Information Download Settings section, ensure that the Enable Patch Information Download check box is checked. By default, this check box appears checked.
3 In the **Patch Information Download Settings** section, enter the details to set up the proxy server. Also, enter the details to set up the download schedule for the patches.

See “Proxy server and download schedule settings options” on page 156.

4 Click **Save Settings**.

See “Configuring SMTP settings for email notifications” on page 29.

See “Viewing the patches available to a host” on page 153.

See “Viewing the details of a patch in the SORT Web site” on page 154.

See “Downloading patch information in offline mode” on page 156.

### Proxy server and download schedule settings options

You must enter the following information to set up the proxy server to connect to the Symantec Web site.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>Enter the name or IP address of the proxy server.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>Enter the port number of the proxy server.</td>
</tr>
<tr>
<td>Proxy User</td>
<td>Enter the user name that you use to access the proxy server.</td>
</tr>
<tr>
<td>Proxy Password</td>
<td>Enter the password that you use to access the proxy server.</td>
</tr>
<tr>
<td>Download Schedule</td>
<td>Choose the appropriate download schedule for the patch that you need.</td>
</tr>
<tr>
<td>Time</td>
<td>Specify the time at which you want to download the patch.</td>
</tr>
</tbody>
</table>

See “Setting up proxy server details to download patch information” on page 155.

### Downloading patch information in offline mode

If Management Server of Veritas Operations Manager is not connected to the Symantec Web site using the Internet and you cannot set up a proxy server for
accessing the Symantec Web site, you can download the patch information in the offline mode.

**Note:** You must use a Windows system to perform this operation.

On the Windows machine, you must download and run the `vos.vbs` script to create the `vos.txt` file. The `vos.txt` file contains the information on patches. You can upload the `vos.txt` file to Veritas Operations Manager Management Server.

**To download patch information in offline mode**

1. Select **Settings > Management Server**.
2. At the bottom of the **Patch Information Download Settings** section, click **Offline Patch Information Download** to display the fields.
3. Click **Download** to download the `vos.vbs` script to your Windows system.
4. Run the `vos.vbs` script on your Windows system to create the `vos.txt` file.
   
   You can use the `cscript /NoLogo vos.vbs` command to create the `vos.txt` file.
5. Browse and select the `vos.txt` file.
6. Click **Upload** to upload the `vos.txt` file to Veritas Operations Manager Management Server

See “Configuring SMTP settings for email notifications” on page 29.

See “Setting up proxy server details to download patch information” on page 155.

See “Viewing the details of a patch in the SORT Web site” on page 154.

See “Viewing the details of a patch in the SORT Web site” on page 154.
Monitoring performance in Veritas Operations Manager

This chapter includes the following topics:

- About Veritas Operations Manager performance graphs
- Viewing the performance graphs for a volume
- Viewing the performance graphs for a host
- Viewing the performance graphs for a disk
- Viewing the performance graphs for an initiator
- Viewing the performance graphs for a file system
- Comparing the performance of volumes
- Comparing the performance of disks
- Comparing the performance of initiators
- Comparing the performance of hosts
- Comparing the performance of file systems

About Veritas Operations Manager performance graphs

In Veritas Operations Manager, you can view the performance of the following objects by using interactive graphs:

- Hosts
You can use the performance graphs in the following ways:

- Select a single object and view graphs of the selected object for multiple performance parameters.
- Select up to five objects and compare the graphs of the selected objects for a single performance parameter.

These graphs are line charts. The X-axis represents the time duration and the Y-axis represents one or more performance parameters. In performance graphs for a single object, the lines that represent the performance parameters are rendered in different colors. In performance graphs for multiple objects, the lines that represent the selected objects are rendered in different colors.

On the performance graphs, you can do the following:

- Specify the duration for which you want to view the performance of one or more objects that you select.
- Specify one or more parameters for which you want to view the performance graphs.
- Move the mouse pointer over the line chart to view performance data. A tooltip is displayed corresponding to the position of the mouse pointer on the graph.
- Change the background color of the performance graphs.

See “Viewing the performance graphs for a volume” on page 161.
See “Viewing the performance graphs for a host” on page 162.
See “Viewing the performance graphs for a disk” on page 163.
See “Viewing the performance graphs for an initiator” on page 164.
See “Viewing the performance graphs for a file system” on page 165.
See “Comparing the performance of volumes” on page 167.
See “Comparing the performance of hosts” on page 170.
See “Comparing the performance of disks” on page 168.
See “Comparing the performance of initiators” on page 169.
See “Comparing the performance of file systems” on page 171.
Viewing the performance graphs for a volume

In Veritas Operations Manager, you can view the performance of a volume by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

**Note:** You can view the performance graphs only for a volume of type VxVM and if the volume belongs to a disk group.

You can specify one of the following durations for which the performance graphs can be rendered:

- Six hours
- 24 hours
- One week
- One month
- One year
- Live (Live data that is refreshed in every five seconds)

You can view the following performance graphs for a volume:

- The Average Read / Write Time graph that displays the average read and write time for the volume for the specified duration.
- The Bytes Written / Read graph that displays the number of bytes written and read on the volume for the specified duration.

To view the performance graphs for a volume

1. In the Veritas Operations Manager console, click **Manage > Hosts**.
2. In the **Hosts** view, click the name of the host and in the detailed view of the host, click on the **Volumes** tab.
3. In the **Volumes** view, do one of the following:
   - Click the name of the volume and in the detailed view of the volume, click on the **Performance** tab.
   - Check the check box for the volume that you want to select and on the top of the **Volumes** table, click **Performance**.
   - Right-click the volume that you want to select and then click **Performance**.
4. On the performance graphs, select one of the time duration options and check the desired check boxes to change the view of the performance graphs.
Viewing the performance graphs for a host

In Veritas Operations Manager, you can view the performance of a host by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

Note: You cannot view the performance graphs for a host on the Windows platform.

You can specify one of the following durations for which the performance graphs can be rendered:

- Six hours
- 24 hours
- One week

You can view the following performance graphs for a host:

- The Free Memory graph that displays the free memory in the host for the specified duration.
- The Average CPU Load graph that displays the average CPU load on the host for the specified duration.

To view the performance graphs for a host

1. In the Veritas Operations Manager console, click Manage > Hosts.
2. In the Hosts view, do one of the following:
   - Click the name of the host and in the detailed view of the host, click on the Performance tab.
   - Check the check box for the host that you want to select and on the top of the Hosts table, click Performance.
Right-click the host that you want to select and then click **Performance**.

3 On the performance graphs, select one of the options to change the duration for which you want to view the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.
See “Comparing the performance of hosts” on page 170.
See “Viewing the performance graphs for a volume” on page 161.
See “Viewing the performance graphs for a disk” on page 163.
See “Viewing the performance graphs for an initiator” on page 164.
See “Viewing the performance graphs for a file system” on page 165.

**Viewing the performance graphs for a disk**

In Veritas Operations Manager, you can view the performance of a disk by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

---

**Note**: You can view the performance graphs only for a disk that VxVM manages and if the disk belongs to a disk group.

You can specify one of the following durations for which the performance graphs can be rendered:

- Six hours
- 24 hours
- One week
- One month
- One year
- Live (Live data that is refreshed in every five seconds)

You can view the following performance graphs for a disk:

- The Average Read / Write Time graph that displays the average read and write time for the disk for the specified duration.
- The Bytes Written / Read graph that displays the number of bytes written and read on the disk for the specified duration.
To view the performance graphs for a disk

1. In the Veritas Operations Manager console, click Manage > Hosts.

2. In the Hosts view, click the name of the host and in the detailed view of the host, click on the Disks tab.

3. In the Disks view, do one of the following:
   - Click the name of the disk and in the detailed view of the disk, click on the Performance tab.
   - Check the check box for the disk that you want to select and on the top of the Disks table, click Performance.
   - Right-click the disk that you want to select and then click Performance.

4. On the performance graphs, select one of the time duration options and check the desired check boxes to change the view of the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.
See “Comparing the performance of disks” on page 168.
See “Viewing the performance graphs for a host” on page 162.
See “Viewing the performance graphs for a volume” on page 161.
See “Viewing the performance graphs for an initiator” on page 164.
See “Viewing the performance graphs for a file system” on page 165.

Viewing the performance graphs for an initiator

In Veritas Operations Manager, you can view the performance of an initiator by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

You can specify one of the following durations for which the performance graphs can be rendered:

- Six hours
- 24 hours
- One week
- One month
- One year
- Live (Live data that is refreshed in every five seconds)

You can view the following performance graphs for an initiator:
- The Average Read / Write Time graph that displays the average read and write time for the initiator for the specified duration.
- The Bytes Written / Read graph that displays the number of bytes written and read on the initiator for the specified duration.
- The Read / Write Errors and Read / Write Queue graph that displays the number of read / write errors and the count of read / write queue for the initiator for the specified duration.

To view the performance graphs for an initiator

1. In the Veritas Operations Manager console, do one of the following:
   - Click Manage > Hosts. Click on the required host.
   - Click Manage > Hosts and click on a host. In the host details view, click on Disks and click on the required disk. Click Paths.
2. Click Initiators.
3. In the Initiators view, do one of the following:
   - Click the name of the initiator and in the detailed view of the initiator, click on the Performance tab.
   - Check the check box for the initiator that you want to select and on the top of the Initiators table, click Performance.
   - Right-click the initiator that you want to select and then click Performance.
4. On the performance graphs, select one of the time duration options and check the desired check boxes to change the view of the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.
See “Comparing the performance of initiators” on page 169.
See “Viewing the performance graphs for a host” on page 162.
See “Viewing the performance graphs for a volume” on page 161.
See “Viewing the performance graphs for a disk” on page 163.
See “Viewing the performance graphs for a file system” on page 165.

Viewing the performance graphs for a file system

In Veritas Operations Manager, you can view the performance of a file system by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.
You can specify one of the following durations for which the performance graphs can be rendered:

- Six hours
- 24 hours
- One week
- One month
- One year

You can view the following performance graph for a file system:

- The Size / Used graph that displays the size and the used space of the file system for the specified duration.

**To view the performance graphs for a file system**

1. In the Veritas Operations Manager console, click **Manage > Hosts**.

2. In the **Hosts** view, click the name of the host and in the detailed view of the host, click on the **File Systems** tab.

3. In the **File Systems** view, do one of the following:
   - Click the name of the file system and in the detailed view of the file system, click on the **Performance** tab.
   - Check the check box for the file system that you want to select and on the top of the **File Systems** table, click **Performance**.
   - Right-click the file system that you want to select and then click **Performance**.

4. On the performance graphs, select one of the time duration options and check the desired check boxes to change the view of the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.

See “Comparing the performance of file systems” on page 171.

See “Viewing the performance graphs for a host” on page 162.

See “Viewing the performance graphs for a volume” on page 161.

See “Viewing the performance graphs for a disk” on page 163.

See “Viewing the performance graphs for an initiator” on page 164.
Comparing the performance of volumes

In Veritas Operations Manager, you can compare the performances of up to five volumes by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

**Note:** You can view the performance graphs only for the volumes of type VxVM and if the volumes belong to a disk group.

You can specify one of the following durations for which the performance graphs can be rendered:

- Six hours
- 24 hours
- One week
- One month
- One year
- Live (Live data that is refreshed in every five seconds)

You can view the following performance graphs for the volumes that you want to compare:

- The Average Read / Write Time graph that displays the average read and write time for the selected volumes for the specified duration.
- The Bytes Written / Read graph that displays the number of bytes written and read on the selected volumes for the specified duration.

**To compare the performance of volumes**

1. In the Veritas Operations Manager console, click **Manage > Hosts**.
2. In the **Hosts** view, click the name of the host and in the detailed view of the host, click on the **Volumes** tab.
3. In the **Volumes** view, check the check boxes for the volumes that you want to compare and do one of the following:
   - On the top of the **Volumes** table, click **Performance**.
   - Right-click one of the selected volumes and then click **Performance**.
4. On the performance graphs, select the desired options to change the view of the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.
Comparing the performance of disks

In Veritas Operations Manager, you can compare the performances of up to five disks by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

**Note:** You can view the performance graphs only for the disks that VxVM manages and if the disks belong to a disk group.

You can specify one of the following durations for which the performance graphs can be rendered:

- Six hours
- 24 hours
- One week
- One month
- One year
- Live (Live data that is refreshed in every five seconds)

You can view the following performance graphs for the disks that you want to compare:

- The Average Read / Write Time graph that displays the average read and write time for the selected disks for the specified duration.
- The Bytes Written / Read graph that displays the number of bytes written and read on the selected disks for the specified duration.

**To compare the performance of disks**

1. In the Veritas Operations Manager console, click **Manage > Hosts**.
2. In the **Hosts** view, click the name of the host and in the detailed view of the host, click on the **Disks** tab.
3. In the **Disks** view, check the check boxes for the disks that you want to compare and do one of the following:
On the top of the Disks table, click Performance.
Right-click one of the selected disks and then click Performance.

4 On the performance graphs, select the desired options to change the view of the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.
See “Viewing the performance graphs for a disk” on page 163.
See “Comparing the performance of volumes” on page 167.
See “Comparing the performance of initiators” on page 169.
See “Comparing the performance of hosts” on page 170.
See “Comparing the performance of file systems” on page 171.

Comparing the performance of initiators

In Veritas Operations Manager, you can compare the performances of up to five initiators by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

You can specify one of the following durations for which the performance graphs can be rendered:

■ Six hours
■ 24 hours
■ One week
■ One month
■ One year
■ Live (Live data that is refreshed in every five seconds)

You can view the following performance graphs for the initiators that you want to compare:

■ The Average Read / Write Time graph that displays the average read and write time for the selected initiators for the specified duration.
■ The Bytes Written / Read graph that displays the number of bytes written and read on the selected initiators for the specified duration.
■ The Read / Write Errors and Read / Write Queue graph that displays the number of read / write errors and the count of read / write queue for the selected initiators for the specified duration.
To compare the performance of initiators

1. In the Veritas Operations Manager console, click Manage > Hosts.

2. In the Hosts view, click the name of the host and in the detailed view of the host, click on the Initiators tab.

3. In the Initiators view, check the check boxes for the initiators that you want to compare and do one of the following:
   - On the top of the Initiators table, click Performance.
   - Right-click one of the selected initiators and then click Performance.

4. On the performance graphs, select the desired options to change the view of the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.
See “Viewing the performance graphs for an initiator” on page 164.
See “Comparing the performance of volumes” on page 167.
See “Comparing the performance of disks” on page 168.
See “Comparing the performance of hosts” on page 170.
See “Comparing the performance of file systems” on page 171.

Comparing the performance of hosts

In Veritas Operations Manager, you can compare the performances of up to five hosts by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

Note: You cannot view the performance graphs for the hosts on the Windows platform.

You can specify one of the following durations for which the performance graphs can be rendered:
- Six hours
- 24 hours
- One week

You can view the following performance graphs for the hosts that you want to compare:
The Available Memory graph that displays the free memory in the selected hosts for the specified duration.

The Average CPU Load graph that displays the average CPU load on the selected hosts for the specified duration.

**To compare the performance of file systems**

1. In the Veritas Operations Manager console, click **Manage > Hosts**.

2. In the **Hosts** view, check the check boxes for the hosts that you want to compare and do one of the following:
   - On the top of the **Hosts** table, click **Performance**.
   - Right-click one of the selected hosts and then click **Performance**.

3. On the performance graphs, select the desired options to change the view of the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.

See “Viewing the performance graphs for a file system” on page 165.

See “Comparing the performance of volumes” on page 167.

See “Comparing the performance of disks” on page 168.

See “Comparing the performance of hosts” on page 170.

See “Comparing the performance of file systems” on page 171.

**Comparing the performance of file systems**

In Veritas Operations Manager, you can compare the performances of up to five file systems by using interactive graphs. These graphs let you specify the duration for which you want to view the performance.

You can specify one of the following durations for which the performance graphs can be rendered:

- Six hours
- 24 hours
- One week
- One month
- One year

You can view the following performance graph for the file systems that you want to compare:
The Size / Used graph that displays the size and the used space of the selected file systems for the specified duration.

To compare the performance of file systems

1. In the Veritas Operations Manager console, click Manage > Hosts.
2. In the Hosts view, click the name of the host and in the detailed view of the host, click on the File Systems tab.
3. In the File Systems view, check the check boxes for the file systems that you want to compare and do one of the following:
   - On the top of the File Systems table, click Performance.
   - Right-click one of the selected file systems and then click Performance.
4. On the performance graphs, select the desired options to change the view of the performance graphs.

See “About Veritas Operations Manager performance graphs” on page 159.
See “Viewing the performance graphs for a file system” on page 165.
See “Comparing the performance of volumes” on page 167.
See “Comparing the performance of disks” on page 168.
See “Comparing the performance of hosts” on page 170.
See “Comparing the performance of initiators” on page 169.
Managing Security groups in Veritas Operations Manager

This chapter includes the following topics:

■ About the security model for Veritas Operations Manager
■ About predefined roles in Veritas Operations Manager
■ Viewing security group details in Veritas Operations Manager
■ Adding security groups to the Veritas Operations Manager domain
■ Modifying the security groups in the Veritas Operations Manager domain
■ Removing security groups from Veritas Operations Manager

About the security model for Veritas Operations Manager

The security model specifies and enforces security policies. In Veritas Operations Manager, the security model is based on the mapping between security groups and roles.

The security model uses the following entities:

■ Security group
■ Role
■ Authentication domain
Veritas Operations Manager lets you combine a role and a scope to specify a predefined role. The following table explains the combination of roles and scopes and the resultant predefined roles:

<table>
<thead>
<tr>
<th>Role and scope</th>
<th>Predefined role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin and Domain (All Business Entities)</td>
<td>Domain Admin</td>
</tr>
<tr>
<td>Admin and Selected Business Entities</td>
<td>Admin</td>
</tr>
<tr>
<td>Operator and Domain (All Business Entities)</td>
<td>Domain Operator</td>
</tr>
<tr>
<td>Operator and Selected Business Entities</td>
<td>Operator</td>
</tr>
<tr>
<td>None</td>
<td>Guest</td>
</tr>
</tbody>
</table>

When a user logs in, Veritas Operations Manager uses an authentication broker to authenticate the user across an authentication domain. If the user is authenticated, Veritas Operations Manager uses the authentication domain name and domain type to determine the security group that can be associated with the user. The security group is mapped to a predefined role.

See “About predefined roles in Veritas Operations Manager” on page 174.

See “Viewing security group details in Veritas Operations Manager” on page 180.

### About predefined roles in Veritas Operations Manager

Veritas Operations Manager lets you combine a role and a scope to specify a predefined role. The following table explains the combination of roles and scopes and the resultant predefined roles:

<table>
<thead>
<tr>
<th>Table 12-1 Summary of predefined roles in Veritas Operations Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role and scope</td>
</tr>
<tr>
<td>Admin and Domain (Entire Domain)</td>
</tr>
<tr>
<td>Admin and Selected Business Entities</td>
</tr>
<tr>
<td>Operator and Domain (Entire Domain)</td>
</tr>
<tr>
<td>Operator and Selected Business Entities</td>
</tr>
<tr>
<td>Guest</td>
</tr>
</tbody>
</table>
In the **New Security Group** panel, you must specify a role and a scope to assign a predefined role to the security group.

Veritas Operations Manager lets you provide the role that you create with the privilege to access the views and reports and perform the operations that are related to out-of-band storage management. To provide the storage administration privileges, you can use the *Allow access to storage views and operations* check box on the **New Security Group** wizard panel.

If you do not select the *Allow access to storage views and operations* check box, the administrators or the operators with the role that you create can only administer the servers. They cannot access the views and reports and perform the operations that are related to out-of-band storage management from the servers that they administer.

**Table 12-2** table explains the role and the scope that you must select to assign a predefined role to security groups.

---

**Note:** You cannot provide any scope to the Guest role. When you select the Guest role, the panel does not display the Scope options.
### Table 12-2  Veritas Operations Manager predefined roles

<table>
<thead>
<tr>
<th>Role and scope</th>
<th>Predefined role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Admin and Domain (Entire Domain) | Domain Admin | A user with the Domain Admin role has complete access to the system and can do the following:  
- Access all managed hosts that are added to Management Server.  
- Access the views and reports and perform the operations that are related to out-of-band storage management.  
- Manage the business entities.  
- Manage the authentication brokers.  
- Manage the security groups.  
- Create the users with the Admin role.  
- Access all Veritas Operations Manager Add-ons.  
- Deploy the packages and patches.  
- Manage all the hosts.  
- Perform all the configurations and the operations on all the VCS cluster.  

**Note:** Only the users with the **Domain Admin** role can create business entities, create security groups, and add hosts to the domain. |
### Table 12-2  Veritas Operations Manager predefined roles (continued)

<table>
<thead>
<tr>
<th>Role and scope</th>
<th>Predefined role</th>
<th>Description</th>
</tr>
</thead>
</table>
| Admin and Selected Business Entities | Admin | A user with the Admin role has restricted access to the managed hosts that are added to Management server. The Admin role is mapped to a security group with one or more business entities. An Admin can do the following:  
- Access all objects in a business entity that is associated with the security group to which the Admin role is mapped.  
- Perform all operations on the objects in a business entity that is associated with the security group to which the Admin role is mapped.  
- Perform the configurations and the operations on the VCS cluster if the cluster is added to the business entity as a base object.  
- Perform the configurations and the operations on the service groups and the associated storage objects if the service group is added to the business entity as a base object.  
An Admin with the privileges to access the storage views and operations can access the views and reports and perform the operations that are related to out-of-band storage management from the objects in the application group to which the Admin role is mapped. |
<table>
<thead>
<tr>
<th>Role and scope</th>
<th>Predefined role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operator and Domain (Entire Domain)</strong></td>
<td>Domain Operator</td>
<td>A user with the Domain Operator role can perform all operations on all the VCS clusters. But, this user is not allowed to make any configuration changes to the VCS clusters. A Domain Operator with the privileges to access the storage views and operations can access the views and reports and perform the operations that are related to out-of-band storage management from the VCS clusters in Veritas Operations Manager. A Domain Operator is provided with the Guest role on the Storage Foundation objects.</td>
</tr>
</tbody>
</table>
### Table 12-2  
Veritas Operations Manager predefined roles (continued)

<table>
<thead>
<tr>
<th>Role and scope</th>
<th>Predefined role</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Operator and Selected Business Entities** | Operator        | A user with the Operator role can do the following:  
- Clear the service groups.  
- Make service groups and storage resources online or offline.  
- Temporarily freeze or unfreeze service groups.  
- Switch the service groups.  
- Autoenable the service groups.  
- Display information on application heartbeat for a service group.  
- Bring the resources online or take them offline.  
- Run an action on the resources.  
- Refresh the information on the resources.  
- Flush the service groups.  
- Flush the resources.  

The operator can perform these tasks based on the clusters or service groups that are added to the business entities as base objects.  

An Operator with the privileges to access the storage views and operations can access the views and reports and perform the operations that are related to out-of-band storage management from the VCS clusters in the application group to which the Operator role is mapped.  

An Operator is provided with the Guest role on the Storage Foundation objects.  

| **Guest**                        | Guest           | The users with the Guest role have read-only access. They cannot perform any tasks in Veritas Operations Manager. |
See “About the security model for Veritas Operations Manager” on page 173.

Viewing security group details in Veritas Operations Manager

The Security Settings view displays the details of the security groups in Veritas Operations Manager. By default, the root security group is mapped to the root authentication group in the primary authentication broker. The root security group is associated with the Domain Admin role.

The following table describes the information that you can view for each security group:

<table>
<thead>
<tr>
<th>Name</th>
<th>Name of the security group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Name of the authentication domain that you have associated with the security group.</td>
</tr>
<tr>
<td>Domain Type</td>
<td>The domain type in the authentication domain of the security group.</td>
</tr>
<tr>
<td>Role</td>
<td>The predefined role that is associated with the security group.</td>
</tr>
</tbody>
</table>

This column displays the following predefined roles based on the Role and the Scope that you have specified in the New Security Group wizard panel:

- Domain Admin
- Admin
- Domain Operator
- Operator
- Guest

Note: You cannot provide any scope to the Guest role.
**Scope**

The scope that is provided to the role, which is part of the security group.

For the Domain Admin and the Domain Operator roles, this field displays the scope as Entire Domain. For the Operator and the Admin roles, this field displays the name of one or more business entities that are used to limit the scope of the roles.

For the Guest role, this field displays the scope as **Entire Domain (Read-only)**.

**Note:** Business entities are associated with the security group only if that security group is mapped to the Admin or the Operator roles.

**Storage Access**

Displays whether the role that is associated with the security group has privileges to access the views and reports and perform the operations that are related to out-of-band storage management.

In the **Security Groups** view, you can do the following:

- Create new security groups.
- Modify the existing security groups.
- Remove the security groups.

**To view the details of security groups**

1. Select **Settings > Security Groups**.
2. In the **Security Groups** view, the details of the security groups in a table.

See “About the security model for Veritas Operations Manager” on page 173.

See “Adding security groups to the Veritas Operations Manager domain” on page 182.

See “Modifying the security groups in the Veritas Operations Manager domain” on page 186.

See “Removing security groups from Veritas Operations Manager” on page 188.
Adding security groups to the Veritas Operations Manager domain

The **New Security Group** wizard panel lets you add a new security group to the Veritas Operations Manager domain.

Veritas Operations Manager lets you combine a role and a scope to specify a predefined role. The following table explains the combination of roles and scopes and the resultant predefined roles:

<table>
<thead>
<tr>
<th>Role and scope</th>
<th>Predefined role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin and Domain (Entire Domain)</td>
<td>Domain Admin</td>
</tr>
<tr>
<td>Admin and Selected Business Entities</td>
<td>Admin</td>
</tr>
<tr>
<td>Operator and Domain (Entire Domain)</td>
<td>Domain Operator</td>
</tr>
<tr>
<td>Operator and Selected Business Entities</td>
<td>Operator</td>
</tr>
<tr>
<td>Guest</td>
<td>Guest</td>
</tr>
</tbody>
</table>

To create a new security group, you must associate an authentication group and an authentication domain with one of the predefined roles in Veritas Operations Manager.

**Note:** You cannot provide any scope to the Guest role. When you select the **Guest** role, the panel does not display the **Scope** options.

To the Admin and the Operator roles, you can provide the rights to administer either all the business entities or a specific set of business entities present in Veritas Operations Manager.

If you want to use an LDAP domain for users belonging to a specific role, you must create a security group that associates the authentication domain and the role.

Veritas Operations Manager lets you provide the role that you create with the privilege to access the views and reports and perform the operations that are related to out-of-band storage management. To provide the storage administration privileges, you can use the **Allow access to storage views and operations** check box on the **New Security Group** wizard panel.

If you do not select the **Allow access to storage views and operations** check box, the administrators or the operators with the role that you create can only administer the servers. They cannot access the views and reports and perform
the operations that are related to out-of-band storage management from the servers that they administer.

The privilege to access the storage views and operations is global in nature. You cannot provide any scope to this privilege. However, you can provide the scope to the role that has the privilege to access the storage views and operations. For example, if you have provided the privilege to access the storage views and operations to the Admin role with the right to administer the business entity \textit{BEhosts\_example} that is based on hosts, the administrators with this role can delve in to the storage views from the hosts that are part of \textit{BEhosts\_example}.

In Veritas Operations Manager, the Dynamic Multipathing (DMP) maintenance operations and the discovery of information on the arrays are directly dependent on the privilege to access the storage views and operations that you have provided to a predefined role.

For more information, refer to the \textit{Veritas™ Operations Manager Administrator's Guide} and the \textit{Veritas™ Operations Manager Storage Insight Add-on for Deep Array Discovery and Mapping User's Guide}.

The name of the security group that you create must match the name of the authentication group present in the authentication domain that you use to create it.

\textbf{Note:} Users with the Domain Admin role can access all the business entities in Veritas Operations Manager.

\section*{To add security groups to the domain}

\begin{enumerate}
\item Select \textit{Settings > Security Groups}.
\item Click \textit{New Security Group}.
\item In the \textit{New Security Group} wizard panel, enter the details and click \textit{OK}.
\item In the \textit{Results} panel that confirms the action, click \textit{OK}.
\end{enumerate}


See “\textit{Viewing security group details in Veritas Operations Manager}” on page 180.

See “\textit{Modifying the security groups in the Veritas Operations Manager domain}” on page 186.

See “\textit{Removing security groups from Veritas Operations Manager}” on page 188.

\section*{New Security Group options}

Use this wizard panel to define the attributes for a new security group.
### Table 12-3  New Security Group panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name       | Name of the security group that you want to create.  
After you enter the name of the security group, click **Check** to verify that the name of the authentication group and the name that you have specified for the security group are the same. Authentication group can be an OS group or a LDAP/Authentication Domain group.  
Veritas Operations Manager displays an icon that indicates that the verification of the name of the security group is in progress. If the authentication group name and the security group name are the same, Veritas Operations Manager displays a green icon. If the authentication group name and the security group name are different, you can view a red icon.  
*Note:* You must ensure that the name of the authentication group and the security group are the same.  
Name of the security group for NT domain must include the domain name on which the group is configured, and the group name.  
The security group name must be entered in the `domain name\group name` format.  
Example: `Machinename\Administrator` |
| Domain     | Name of the authentication domain that you want to associate with the security group.  
You can choose the domain names from the drop-down list. The drop-down list contains all the authentication domains that are in the enabled state. |
| Role       | Choose any of the following roles that you want to associate with the security group:  
- **Admin**  
- **Operator**  
- **Guest** |
Table 12-3  New Security Group panel options *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access to storage views and operations</td>
<td>Select this check box if you want to provide the role that you create with the privileges to access the views and reports and perform the operations that are related to out-of-band storage management. If you have not selected this check box, the administrators or operators with the role that you create can only administer the servers. They cannot access the views and reports and perform the operations that are related to out-of-band storage management from the servers that they administer.</td>
</tr>
<tr>
<td>Scope</td>
<td>Choose any of the following options to provide scope to the roles that you have specified:</td>
</tr>
<tr>
<td></td>
<td>■ Entire Domain</td>
</tr>
<tr>
<td></td>
<td>■ Selected Business Entities</td>
</tr>
<tr>
<td></td>
<td>If you choose the scope as <em>Selected Business Entities</em>, the panel displays all the business entities present in Veritas Operations Manager. To limit the scope of the role to one or more specific business entities, you must associate them with the security group. Check the check box on the left side of each of the business entities to associate them with the security group that you create.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You cannot provide any scope to the Guest role. When you select the <em>Guest</em> role, the panel does not display the Scope options.</td>
</tr>
</tbody>
</table>

See “*Adding security groups to the Veritas Operations Manager domain*” on page 182.
Modifying the security groups in the Veritas Operations Manager domain

The Edit Access Control wizard panel lets you modify the security groups in the Veritas Operations Manager domain. You can modify the role and the scope that are associated with a security group.

You cannot modify the security group name or the authentication domain that is associated with the security group.

To modify the security groups in a domain

2. Check the check box for the security group that you want to modify and click Edit Access Control.
3. In the Edit Access Control wizard panel, modify the role and the scope as required and click OK.
   
   See “Edit Access Control options” on page 186.

4. In the Results panel that confirms the action, click OK.

See “About the security model for Veritas Operations Manager” on page 173.

See “Adding security groups to the Veritas Operations Manager domain” on page 182.

See “Removing security groups from Veritas Operations Manager” on page 188.

Edit Access Control options

Use this wizard panel to modify the role and the scope that are associated with the security group.

Note: You cannot modify the name of the security group and the authentication domain that is associated with the security group.
### Table 12-4  Edit Access Control panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the security group. You cannot edit this field. You can click <strong>Check</strong> to verify that the security group that you have created still exists in the authentication domain. Veritas Operations Manager displays an icon that indicates that the verification of the security group is in progress. If the security group exists in the authentication domain, Veritas Operations Manager displays a green icon. If the security group no longer exists in the authentication domain, you can view a red icon.</td>
</tr>
<tr>
<td>Domain</td>
<td>Displays the authentication domain that is associated with the security group. You cannot edit this field.</td>
</tr>
<tr>
<td>Role</td>
<td>Choose the new role that you want to associate with the security group.</td>
</tr>
<tr>
<td>Allow access to storage views and operations</td>
<td>Select or clear this check box to modify the privileges that you have provided to the role to access the views and reports and perform the operations that are related to out-of-band storage management.</td>
</tr>
</tbody>
</table>
| Scope                  | Choose any of the following options to provide new scope to the roles that you have specified:  
  - **Entire Domain**  
  - **Selected Business Entities**  
  If you choose the scope as **Selected Business Entities**, check the check box on the left side of the business entities that you want to associate with the security group.  
  **Note:** You cannot provide any scope to the Guest role. When you select the **Guest** role, the panel does not display the Scope options. |
Removing security groups from Veritas Operations Manager

The Remove Security Group wizard panel lets you remove one or more security groups from Veritas Operations Manager. When you remove a security group, the association of the authentication group and authentication domain with the role and application groups is also removed.

**Note:** You cannot remove the root security group that is mapped to the root authentication group of the primary Authentication Broker.

To remove security groups from Veritas Operations Manager

1. Select **Settings > Security Groups**.
2. Select one or more security groups that you want to remove and click **Remove Security Group**.
3. In the **Remove Security Group** wizard panel to confirm whether you need to remove the security groups that you have selected, click **Yes**.
4. In the **Results** panel that confirms that you removed the selected security groups, click **OK**.

See “Modifying the security groups in the Veritas Operations Manager domain” on page 186.
Managing Business Entities in Veritas Operations Manager

This chapter includes the following topics:

- About managing business entities in Veritas Operations Manager
- About security privileges required to manage business entities
- Creating composite business entities in Veritas Operations Manager
- Creating application business entities in Veritas Operations Manager
- Creating organization business entities in Veritas Operations Manager
- Viewing the business entities in Veritas Operations Manager
- Editing an application business entity
- Editing an organization business entity
- Removing business entities
- Adding storage or high availability objects to an existing business entity
- Making a business entity available to the security groups in Veritas Operations Manager
- Setting the extended attributes on a business entity
About managing business entities in Veritas Operations Manager

In Veritas Operations Manager, you can create business entities to group base objects for the purpose of reporting and alerting. Based on the type of included objects, Veritas Operations Manager version 4.0 provides two types of business entities: application business entities and organization business entities.

Application business entities can be used to group one or more of the following base object types:
- Databases
- Hosts
- Service Groups
- File systems
- Disk groups
- Enclosures
- Clusters
- Exchange Servers

Organization business entities can be used to group only managed hosts.

**Composite business entities:** With composite business entities, you can group one or more business entities of similar type, and treat them as a single object. This mechanism lets you perform various tasks collectively on the added business entities. You can create two types of composite business entities.

- Application composite business entity: It contains only the application business entities.
- Organization composite business entity: It contains only the organization business entities.

You can perform the following operations related to business entities:
- Create new business entities.
- Modify business entities.
- Change the security priorities of business entities.
- Delete business entities.

See “About security privileges required to manage business entities” on page 191.

See “Editing an application business entity” on page 203.
About security privileges required to manage business entities

In Veritas Operations Manager, business entities are associated with the security groups to provide access rights to the users with the Domain Admin role so that they can access specific hosts and storage devices. Domain administrators can perform all operations on business entities.

Restricted administrators can also perform some operations on business entities within the following rules:

- They can remove base hosts from an application business entity if they have administrator privileges for the business entity.
- They can add any host that they have administrator privileges on, as a base host to an application business entity. This includes the hosts that are added to other application or organization business entities that the restricted administrator has administrator privileges on.
- They cannot add hosts to organization business entities, or remove hosts from them.
- They cannot edit application business entities.
- They cannot delete application business entities even if they have administrator privileges for them.

See “Adding security groups to the Veritas Operations Manager domain” on page 182.

See “Modifying the security groups in the Veritas Operations Manager domain” on page 186.

Creating composite business entities in Veritas Operations Manager

With composite business entities, the administrator can group one or more business entities of similar type, and treat them as a single object. This mechanism lets you perform various tasks collectively on the added business entities. You can create two types of composite business entities.

- Application composite business entity: It contains only the application business entities.
- Organization composite business entity: It contains only the organization business entities.
To create a composite business entity

1. In the Veritas Operations Manager console, select Manage > Business Entities.

2. In the Business Entities view, at the top of the table that lists the business entities, click New Composite Business Entity.

3. In the Composite Business Entity Attributes panel, enter the details, and click Next.

   See “Composite Business Entity Attributes options” on page 192.

4. In the Select Business Entity panel, select one or more business entities that you want to add to the composite business entity, and click Next.

   See “Select Business Entity panel options” on page 193.

5. In the Business Entity Summary panel, review your selections and click Finish.

   See “Composite Business Entity Summary panel options” on page 193.

6. In the Results panel that confirms the creation of the composite business entity, click OK.

   See “Creating application business entities in Veritas Operations Manager” on page 194.

   See “Creating organization business entities in Veritas Operations Manager” on page 200.

Composite Business Entity Attributes options

Use this panel to create a new composite business entity. A composite business entity lets you further group business entities of same type. For example, you can create a composite business entity of type application, and add multiple application business entities to it.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the composite business entity. In this field, you can enter up to 255 characters. Example: Production Business Entity</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this composite business entity. In this field, you can enter up to 255 characters. Example: All servers and storage that are associated with the Production Business Entity.</td>
</tr>
</tbody>
</table>
Table 13-1 Composite Business Entity Attributes options *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Type  | Select the type of the composite business entity.  
   - **Application**: The application type of composite business entity can contain one or more application business entities.  
   - **Organization**: The organization type of composite business entity can contain one or more organization business entities. |

See “Creating composite business entities in Veritas Operations Manager” on page 191.

**Select Business Entity panel options**

Use this panel to add one or more business entities to the new composite business entity. For a composite business entity of application type, only application business entities are available for the selection. Similarly, if you create a composite business entity of organization type, only organization business entities are available for the selection.

Table 13-2 Select Business Entity options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the business entity. Select the desired business entity that you want to add to the composite business entity.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description for the business entity.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the present state of the business entity.</td>
</tr>
</tbody>
</table>

See “Creating composite business entities in Veritas Operations Manager” on page 191.

**Composite Business Entity Summary panel options**

Use this panel to review the contents, and the attributes of the composite business entity before creating it.

See “Creating composite business entities in Veritas Operations Manager” on page 191.
Creating application business entities in Veritas Operations Manager

With application business entities, administrators can treat a collection of objects as a single group.

You can create the application business entities based on the following base objects:
- Databases
- Exchange Servers
- Hosts
- File systems
- Disk groups
- Clusters
- Service groups
- Enclosures

For each base object, its dependencies (associated objects) are discovered. These include:
- Databases
- Exchange Servers
- Clusters
- Service groups
- Replication
- Hosts
- File systems
- Disk groups
- Volumes
- Disks
- Initiators
- Enclosures

When generating Veritas Operations Manager reports, you can specify an application business entity to run the report on. The users with domain administrator role can manage the business entities in Veritas Operations Manager.
To create an application business entity

1. Select Manage > Business Entities.

2. In the Business Entities view, at the top of the table that lists the business entities, click New Business Entity.

3. In the Business Entity Attributes panel, enter the details and click Next. See “Business Entity Attributes options” on page 196.

4. In the Select Base Object Types panel, select one or more available items and click Next.

   Each of the base object types that you select displays an associated Select Base item panel from which you can select items of that type.

   See “Select Base Object Types options” on page 197.

5. In the Select Base item panels, do the following:
   - If the Select Base Databases panel appears, select one or more databases and click Next.
     See “Select Base Databases options” on page 197.
   - If the Select Base Exchange Servers panel appears, select one or more enclosures and click Next.
     See “Select Base Exchange Servers options” on page 200.
   - If the Select Base Clusters panel appears, select one or more clusters and click Next.
     See “Select Base Clusters options” on page 198.
   - If the Select Base Service Groups panel appears, select one or more service groups and click Next.
     See “Select Base Service Groups options” on page 199.
   - If the Select Base Hosts panel appears, select one or more hosts and click Next.
     See “Select Base Hosts options” on page 198.
   - If the Select Base File Systems panel appears, select one or more file systems and click Next.
     See “Select Base File Systems options” on page 199.
   - If the Select Base Disk Groups panel appears, select one or more disk groups and click Next.
     See “Select Base Disk Groups options” on page 198.
   - If the Select Base Enclosures panel appears, select one or more enclosures and click Next.
     See “Select Base Enclosures options” on page 199.
6 In the Business Entity Summary panel, review your selections and click Finish.
See “Business Entity Summary options” on page 199.

7 In the Results panel that confirms the creation of the application business entity, click OK.
See “Editing an application business entity” on page 203.
See “Making a business entity available to the security groups in Veritas Operations Manager” on page 210.
See “Adding storage or high availability objects to an existing business entity” on page 209.

Business Entity Attributes options
Use this panel to create a business entity. Veritas Operations Manager automatically determines the resources that can belong to a business entity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the business entity. In this field, you can enter up to 255 characters. Example: Accounts Receivable</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this business entity. In this field, you can enter up to 255 characters. Example: All servers and storage that is associated with the Accounts Receivable billing system.</td>
</tr>
</tbody>
</table>
| Type     | Select one of the following types of business entity to create:  
- **Application**: A custom application to show associated objects and faults. More resource intensive, so should be limited to specifying less than 100 base objects.  
- **Organization**: A group of logically associated hosts (e.g. by Admin, by Team, by Datacenter). Less resource intensive, and can include potentially thousands of base hosts. |

See “Creating application business entities in Veritas Operations Manager” on page 194.
See “Creating organization business entities in Veritas Operations Manager” on page 200.
Select Base Object Types options

Use this wizard panel to specify the type of base objects on which the new business entity is to be predicated on. Base objects determine the other objects in the business entity. All other objects that are associated with the base object are included automatically to the business entity.

For example, you might choose a host to be the base object. Then, all the objects that are associated with the hosts are added to the business entity.

**Table 13-4** Select Base Object Types panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>You can check the check box for one or more of the following application types to add them as base objects.</td>
</tr>
<tr>
<td></td>
<td>• Databases</td>
</tr>
<tr>
<td></td>
<td>• Exchange Servers</td>
</tr>
<tr>
<td>HA-DR</td>
<td>You can check the check box for one or more of the following HA-DR objects to add them as base objects.</td>
</tr>
<tr>
<td></td>
<td>• Clusters</td>
</tr>
<tr>
<td></td>
<td>• Service Groups</td>
</tr>
<tr>
<td>Servers</td>
<td>You can check the check box for one or more of the following server types to add them as base objects.</td>
</tr>
<tr>
<td></td>
<td>• Hosts</td>
</tr>
<tr>
<td></td>
<td>• File Systems</td>
</tr>
<tr>
<td></td>
<td>• Disk Groups</td>
</tr>
<tr>
<td>Storage</td>
<td>You can check the check box for <strong>Enclosures</strong> to add it as the base object.</td>
</tr>
</tbody>
</table>

See “Creating application business entities in Veritas Operations Manager” on page 194.

Select Base Databases options

Use this wizard panel to select one or more databases as base objects for the business entity.

**Table 13-5** Select Base Databases

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Table</td>
<td>Select one or more databases to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>
Select Base Clusters options

Use this wizard panel to select the base clusters for the business entity.

Table 13-6  Select Base Clusters options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clusters Table</td>
<td>Select one or more clusters to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

Select Base Hosts options

Use this wizard panel to select the base hosts for the business entity.

Table 13-7  Select Base Hosts

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Table</td>
<td>Select one or more hosts to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

Select Base Disk Groups options

Use this wizard panel to select the base disk groups for the business entity.

Table 13-8  Select Base Disk Groups

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Group Table</td>
<td>Select one or more disk groups to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Creating application business entities in Veritas Operations Manager” on page 194.
Select Base File Systems options

Use this wizard panel to select the file systems for the business entity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System Table</td>
<td>Select one or more file systems to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Creating application business entities in Veritas Operations Manager” on page 194.

Business Entity Summary options

Use this wizard panel to review the contents and attributes of the business entity before creating it.

See “Creating application business entities in Veritas Operations Manager” on page 194.

Select Base Service Groups options

Use this wizard panel to select the base service groups for the business entity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Group Table</td>
<td>Select one or more service groups to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Creating application business entities in Veritas Operations Manager” on page 194.

Select Base Enclosures options

Use this wizard panel to select the base enclosures for the business entity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enclosures Table</td>
<td>Select one or more enclosures to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>
See “Creating application business entities in Veritas Operations Manager” on page 194.

Select Base Exchange Servers options

Use this wizard panel to select the base Exchange Servers for the business entity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Servers Table</td>
<td>Select one or more exchange servers to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

Creating organization business entities in Veritas Operations Manager

With organization business entities, administrators can treat a collection of hosts as a single group. You can create organization business entities based on only the hosts in the Management Server domain.

When generating Veritas Operations Manager reports, you can scope the report to be run for an organization business entity. The users with domain administrator role can manage the business entities in Veritas Operations Manager.

To create an organization business entity

1  Select Manage > Business Entities.
2  In the Business Entities view, at the top of the table that lists the business entities, click New Business Entity.
3  In the Business Entity Attributes panel, enter the details and click Next. See “Business Entity Attributes options” on page 196.
4  In the Select Base Hosts panel, select one or more hosts and click Next. See “Select Base Hosts options” on page 198.
5  In the Business Entity Summary panel, review your selections and click Finish. See “Business Entity Summary options” on page 199.
6  In the Results panel that confirms the creation of the organization business entity, click OK.

See “Editing an organization business entity” on page 208.
See “Making a business entity available to the security groups in Veritas Operations Manager” on page 210.

Viewing the business entities in Veritas Operations Manager

In Veritas Operations Manager, you can view all the business entities currently present in the datacenter.

You can view the following details of the business entities in this table:

- **Name**: Name of the business entity.
- **Description**: Information that you have entered when you created the business entity.
- **State**:
  - For application business entities, the state of the base objects and their dependencies is displayed. The state is based on the faults and the risks on the base objects and their associated objects. If these objects have faults, the state of the business entity is displayed as **Faulted**. If the base objects and their associated objects are at risks, the state of the business entity is displayed as **At Risk**.
  - For organization business entities, the state is displayed as **Healthy**, **At Risk**, or **Faulted**. A **Healthy** state indicates that none of the base hosts are faulted, or at risk. **At Risk** indicates that some, but not all, hosts are faulted, or at least one base host is at risk. **Faulted** indicates that all the base hosts are faulted.
- **Type**: Type of the business entity. It can be a Business Entity, or a Composite Business Entity. A composite business entity lets you group one or more business entities of similar type. A composite business entity is a container to which you can add your business entities. This mechanism lets you perform various tasks collectively on a group of business entities. Based on the type of included objects, both types of business entities can be created as either **Application** type, or **Organization** type.
  - A composite business entity of type **Application** must contain only application business entities. Similarly, a composite business entity of type **Organization** must contain only organization business entities.
- **Admin Access**: Displays whether the logged on user has administrator access to the hosts that are associated with that business entity.
- **Last Updated**: Date when the owner of the business entity made a configuration change to the group.
Use the provided dynamic search filter to search existing business entities in the
datacenter. You can filter the business entities list based on the state of the
business entities - **Faulted**, **At Risk**, or **Healthy**. You can also filter the list based
on the type of the business entities - **Application** or **Organization**.

In this view, you can perform the following operations on a business entity:

- Edit a business entity
- Delete a business entity
- Set the extended attributes for a business entity
- Run the high availability fire drill for a business entity
- Run the disaster recovery fire drill for a business entity
- Enable organization entity for capacity planning (Available only if the Veritas
  Operations Manager LDom Capacity Management Add-on is enabled)
- Disable organization entity for capacity planning (Available only if the Veritas
  Operations Manager LDom Capacity Management Add-on is enabled)
- Start a business entity (Available only if the Veritas Operations Manager
  Business Entity Operations Add-on is enabled)
- Stop a business entity (Available only if the Veritas Operations Manager
  Business Entity Operations Add-on is enabled)
- Configure the start and the stop operations for an application business entity
  (Available only if the Veritas Operations Manager Business Entity Operations
  Add-on is enabled)
- Change the security configurations of a business entity

**To view the business entities in Veritas Operations Manager**

- In the Veritas Operations Manager console, click **Manage > Business Entities**.

See “Creating application business entities in Veritas Operations Manager”
on page 194.

See “Editing an application business entity” on page 203.

See “Removing business entities” on page 209.

See “Making a business entity available to the security groups in Veritas Operations
Manager” on page 210.
Editing an application business entity

The administrators can edit the content of an application business entity by modifying the selection of the base objects, and their dependencies on the business entities.

To edit an application business entity

1. Select Manage > Business Entities.

2. In the Business Entities view, do one of the following:
   - Select the application business entity that you want to edit and click Edit Business Entity.
   - Right-click the application business entity and from the submenu, select Edit Business Entity.

3. In the Business Entity Attributes panel, modify the details and click Next.
   See “Business Entity Attributes options” on page 204.

4. In the Select Base Object Types panel, select one or more of the available items to modify the selection and click Next.
   Each of the base object types you select displays an associated Select Base item panel. You can select the desired items from the list. For instance, under Applications base object type, you can select Database and Exchange Servers.
   See “Select Base Object Types options” on page 204.

5. In the Select Base item panels, do the following:
   - If the Select Base Databases panel appears, select one or more databases to modify the selection and click Next.
     See “Select Base Databases options” on page 205.
   - If the Select Base Exchange Servers panel appears, select one or more disk groups to modify the selection and click Next.
     See “Select Base Exchange Servers options” on page 207.
   - If the Select Base Clusters panel appears, select one or more clusters to modify the selection and click Next.
     See “Select Base Clusters options” on page 205.
   - If the Select Base Service Groups panel appears, select one or more service groups to modify the selection and click Next.
     See “Select Base Service Groups options” on page 206.
   - If the Select Base Hosts panel appears, select one or more hosts to modify the selection and click Next.
     See “Select Base Hosts options” on page 206.
If the Select Base File Systems panel appears, select one or more file systems to modify the selection and click Next. See “Select Base File Systems options” on page 206.

If the Select Base Disk Groups panel appears, select one or more disk groups to modify the selection and click Next. See “Select Base Disk Groups options” on page 207.

If the Select Base Enclosures panel appears, select one or more disk groups to modify the selection and click Next. See “Select Base Enclosures options” on page 207.

6 In the Business Entity Summary panel, review your modified selections and click Finish.

See “Business Entity Summary” on page 208.

7 In the Results panel, click OK.

See “Viewing the business entities in Veritas Operations Manager” on page 201.

See “Removing business entities” on page 209.

See “Adding storage or high availability objects to an existing business entity” on page 209.

Business Entity Attributes options

Use this wizard panel to modify the name and the description of a business entity.

Table 13-13 Business Entity Attributes options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Modify the name of the business entity. You can enter up to 255 characters in this field.</td>
</tr>
<tr>
<td>Description</td>
<td>Modify the description for the business entity. You can enter up to 255 characters in this field.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base Object Types options

Use this wizard panel to modify the selection of the type of objects on which the new business entity is based.
Table 13-14  Select Base Object Types options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Modify the selection of one or more of the following application types to include or exclude them as base objects.</td>
</tr>
<tr>
<td></td>
<td>■ Databases</td>
</tr>
<tr>
<td></td>
<td>■ Exchange Servers</td>
</tr>
<tr>
<td>HA-DR</td>
<td>Modify the selection of one or more of the following HA-DR objects to include or exclude them as base objects.</td>
</tr>
<tr>
<td></td>
<td>■ Clusters</td>
</tr>
<tr>
<td></td>
<td>■ Service Groups</td>
</tr>
<tr>
<td>Servers</td>
<td>Modify the selection of one or more of the following server types to include or exclude them as base objects.</td>
</tr>
<tr>
<td></td>
<td>■ Hosts</td>
</tr>
<tr>
<td></td>
<td>■ File Systems</td>
</tr>
<tr>
<td></td>
<td>■ Disk Groups</td>
</tr>
<tr>
<td>Storage</td>
<td>Modify the selection to include or exclude Enclosures as the base object.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base Databases options

Use this wizard panel to modify the selection of base database(s) for the business entity.

Table 13-15  Select Base Databases options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Table</td>
<td>Select one or more databases to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base Clusters options

Use this wizard panel to modify the selection of clusters for the business entity.
Select Base Clusters options

Use this wizard panel to modify the selection of the base clusters for the business entity.

Table 13-16 Select Base Clusters options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Clusters Table</td>
<td>Select one or more clusters to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base Hosts options

Use this wizard panel to modify the selection of the base hosts for the business entity.

Table 13-17 Select Base Hosts panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Table</td>
<td>Select one or more hosts to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base Service Groups options

Use this wizard panel to modify the selection of the base service groups for the business entity.

Table 13-18 Select Base Service Groups options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Group Table</td>
<td>Select one or more service groups to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base File Systems options

Use this wizard panel to modify the selection of the file systems for the business entity.
Table 13-19  Select Base File Systems options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System Table</td>
<td>Select one or more file systems to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base Disk Groups options

Use this wizard panel to modify the selection of the base disk groups for the business entity.

Table 13-20  Select Base Disk Groups panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk group Table</td>
<td>Select one or more disk groups to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base Enclosures options

Use this wizard panel to modify the selection of the base enclosures for the business entity.

Table 13-21  Select Base Enclosures panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enclosures Table</td>
<td>Select one or more enclosures to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>

See “Editing an application business entity” on page 203.

Select Base Exchange Servers options

Use this wizard panel to modify the selection of the base exchange servers for the business entity.
Business Entity Summary

Use this wizard panel to review the modified contents and attributes of the business entity.

See “Editing an application business entity” on page 203.

Editing an organization business entity

The administrators can edit the content of an organization business entity by modifying the selection of the associated hosts.

To edit an organization business entity

1. Select Manage > Business Entities.
2. In the Business Entities view, do one of the following:
   - Select the organization business entity that you want to edit and click Edit Business Entity.
   - Right-click the organization business entity and from the submenu, select Edit Business Entity.
3. In the Business Entity Attributes panel, modify the details and click Next.
   See “Business Entity Attributes options” on page 204.
4. In the Select Base Hosts panel, select one or more hosts to modify the selection and click Next.
   See “Select Base Hosts options” on page 206.
5. In the Business Entity Summary panel, review your modified selections and click Finish.
   See “Business Entity Summary” on page 208.
6. In the Results panel, click OK.
   See “Viewing the business entities in Veritas Operations Manager” on page 201.
   See “Removing business entities” on page 209.

Table 13-22  Select Base Exchange Servers options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Servers Table</td>
<td>Select one or more exchange servers to include as base objects for the business entity.</td>
</tr>
</tbody>
</table>
Removing business entities

You can use the **Delete Business Entity** wizard panel to remove a business entity from Veritas Operations Manager.

**To remove business entities**

1. Select **Manage > Business Entities**.

2. In the **Business Entities** view, select the business entity that you want to remove and do one of the following:
   - Click **More > Delete Business Entity**.
   - Right-click the business entity and from the submenu, select **Delete Business Entity**.

3. In the **Delete Business Entity** wizard, click **Yes**.

4. In the **Results** panel, click **OK**.

See “Creating application business entities in Veritas Operations Manager” on page 194.

See “Editing an application business entity” on page 203.

See “Making a business entity available to the security groups in Veritas Operations Manager” on page 210.

See “Adding storage or high availability objects to an existing business entity” on page 209.

Adding storage or high availability objects to an existing business entity

You can add storage and high availability objects to the business entity that is present in Veritas Operations Manager.

**To add storage and high availability objects to an existing business entity**

1. To add one or more storage or high availability objects to an existing business entity, navigate to where you can view object. For example, to add hosts to the business entity, select **Manage > Hosts**.

2. Select the check box for the object.

3. At the top of the table that displays objects, click **Add to Business Entity**.
4 In the Add to Business Entity panel, enter the details and click OK. See “Add to Business Entity options” on page 210.

5 In the Results panel, click OK.

Add to Business Entity options

Use this panel to add the selected object to an existing business entity.

Table 13-23 Add to Business Entity options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Business Entity</td>
<td>Select the business entity to which the selected object is to be added.</td>
</tr>
</tbody>
</table>

See “Adding storage or high availability objects to an existing business entity” on page 209.

Making a business entity available to the security groups in Veritas Operations Manager

You can use the Change Permissions wizard panel to provide permissions to one or more security groups to access a business entity.

You can use the security groups to provide access to specific hosts in a business entity to the users with the Domain Admin role.

To make a business entity available to the security groups

1 Select Manage > Business Entities.

2 In the Business Entities view, you can do one of the following:

   ■ Select the business entity that you want to access using the security groups and click More > Change Permissions. Alternatively, you can right-click the business entity and from the submenu, select Change Permissions.

   ■ Click the name of the business entity to view its details. In the details view of the business entity, click the tab Permissions. Under the Permissions tab, click Change Permissions.

3 In the Change Permissions for business entity name panel, do one of the following and click OK.
To provide access permissions, select the check box corresponding the security group.

To remove access permissions, clear the check box corresponding to selected security group.

See “Change Permissions options” on page 211.

4 In the Results panel, click OK.

See “Business Entity Attributes options” on page 196.

See “Editing an application business entity” on page 203.

See “Removing business entities” on page 209.

See “Adding storage or high availability objects to an existing business entity” on page 209.

Change Permissions options

Use this panel to select the security groups to provide permissions to access the business entities. Under Select Security Groups, you can view the table that lists all the security groups that are available in Veritas Operations Manager.

In the table, you can view the following details of the security groups:

- Name of the security group.
- Name of the authentication domain that is associated with the security group.
- Type of the authentication domain that is associated with the security group.
- Role that is associated with the security group.

See “Making a business entity available to the security groups in Veritas Operations Manager” on page 210.

Setting the extended attributes on a business entity

Veritas Operations Manager lets you apply the value of an extended attribute on a business entity. You can select the base object type of the business entity to apply the extended attribute value. Setting the extended attribute on the base business entity applies the extended attributes value to all the objects that are associated with the base object type. Also, you can select an object type that is related to the base object type of the business entity to define the attributes on all the objects that are associated with the object type.
To set the extended attributes on a business entity

1. In Veritas Operations Manager console, select Manage > Business Entities.
2. In the Business Entities view, select the check box on the left side of the row that represents the business entity for which you want to set the extended attributes.
3. At the top of the business entity table, select More > Set Extended Attribute.
4. In the Select base object type panel, enter the required details and click Next.
   See “Select base object type options” on page 212.
5. In the Select related object types panel, select the object types on which you want to define the extended attribute, which is set for the base object type, and click Finish.
   See “Select related object types options” on page 213.
6. In the Result panel that confirms the extended attribute is successfully set on the business entity, click OK.
   See “Setting values to the extended attributes on one or more objects” on page 353.
   See “Modifying the extended attributes value on an object” on page 354.

Select base object type options

Use this panel to select the base object type of the business entity, which lets you apply the extended attribute value to all the objects that are associated with the base business entity.

Note: On the Select base object type panel, you can select only one object type at a time.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Type</td>
<td>Select the base object type of the business group for which you want to set the extended attribute value.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Select the extended attribute that you want to set for the business entity.</td>
</tr>
</tbody>
</table>
Table 13-24  Select base object type panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Enter the value for the extended attribute that you want to apply to all the objects that are associated with the base business entity.</td>
</tr>
</tbody>
</table>

See “Setting the extended attributes on a business entity” on page 211.

Select related object types options

Use this panel to specify the object types on which you want to define the extended attribute that you have set on the business entity.

Table 13-25  Select related object types panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Type</td>
<td>Select the object type on which you want to define the extended attribute.</td>
</tr>
</tbody>
</table>

See “Setting the extended attributes on a business entity” on page 211.
Managing Business Entities in Veritas Operations Manager

Setting the extended attributes on a business entity
Managing Authentication Brokers in Veritas Operations Manager

This chapter includes the following topics:

■ About managing Authentication Brokers in the Veritas Operations Manager domain
■ About managing domains associated with an Authentication Broker in Veritas Operations Manager
■ Viewing the details of the Authentication Brokers and the domains associated with them
■ Adding secondary Authentication Brokers to the Veritas Operations Manager domain
■ Refreshing the information associated with the Authentication Brokers
■ Removing the Authentication Brokers from the Veritas Operations Manager domain
■ Configuring Lightweight Directory Access Protocol-based authentication on the Management Server host
■ Removing Lightweight Directory Access Protocol or Active Directory configuration from the primary Authentication Broker
■ Enabling the authentication domains associated with an Authentication Broker
■ Disabling the authentication domains associated with an Authentication Broker
About managing Authentication Brokers in the Veritas Operations Manager domain

An Authentication Broker is an intermediate registration and certification authority that can authenticate clients including users or services.

In Veritas Operations Manager, an Authentication Broker has one or more authentication domains that authenticate users.

Veritas Operations Manager contains the following types of Authentication Brokers:

- Primary Authentication Broker
- Secondary Authentication Brokers

Primary Authentication Broker is installed on Management Server. You configure it when you configure Management Server.

**Note:** VRTSatServer6.0 is the primary Authentication Broker on Management Server. VRTSat Client 6.0 enables communication between managed hosts.

The Authentication Broker that you add to Veritas Operations Manager is known as secondary Authentication Broker. You can add one or more Secondary Authentication Brokers to the Veritas Operations Manager domain.

**Note:** Only the users with the Domain Admin role can manage Authentication Brokers in Veritas Operations Manager.

Veritas Operations Manager lets you do the following:

- Add one or more secondary Authentication Brokers to the Veritas Operations Manager domain.
- Refresh Authentication Brokers.
- Remove secondary Authentication Brokers from the Veritas Operations Manager domain.

You can also manage the domains that are associated with Authentication Brokers in Veritas Operations Manager.


See “Adding secondary Authentication Brokers to the Veritas Operations Manager domain” on page 219.
See “Refreshing the information associated with the Authentication Brokers” on page 222.

See “Removing the Authentication Brokers from the Veritas Operations Manager domain” on page 222.

About managing domains associated with an Authentication Broker in Veritas Operations Manager

The **Authentication Brokers** view lets you select an Authentication Broker to view the authentication domains that are associated with it. By default, the primary Authentication Broker is selected. Under **Domains**, Veritas Operations Manager lists the authentication domains that are associated with the selected Authentication Broker.

Veritas Operations Manager lets you manage the authentication domains that are associated with the Authentication Brokers. Only the users with the Domain Admin role can manage Authentication Brokers in Veritas Operations Manager.

Veritas Operations Manager supports the authentication mechanism that is configured in the operating system, including Pluggable Authentication Modules (PAM), Network Information Service (NIS), or NIS+, with the exception of multi-factor authentication mechanisms. In addition to the native operating system authentication, Veritas Operations Manager supports Lightweight Directory Access Protocol (LDAP) and Active Directory (AD).

In the Veritas Operations Manager log in page, you can view the following domain types:

- unixpwd
- Network (NT) Domain
- LDAP

See “About managing Authentication Brokers in the Veritas Operations Manager domain” on page 216.

See “Viewing the details of the Authentication Brokers and the domains associated with them” on page 218.


See “Removing Lightweight Directory Access Protocol or Active Directory configuration from the primary Authentication Broker” on page 228.

See “Enabling the authentication domains associated with an Authentication Broker” on page 229.
See “Disabling the authentication domains associated with an Authentication Broker” on page 230.

**Viewing the details of the Authentication Brokers and the domains associated with them**

The **Security Settings** view lets you view the Authentication Brokers and the authentication domains that are associated with them.

Under **Authentication Brokers**, you can view the list of primary and secondary Authentication Brokers in the Veritas Operations Manager domain. You can view the following details for each Authentication Broker:

- **Broker Name**
- **Name of the Authentication Broker**
- **Port No**
- **Port number on which the Authentication Broker is configured to run**

If you select an Authentication Broker, you can view the authentication domains that are associated with it under **Domains**. By default, the primary Authentication Broker is selected in the list of Authentication Brokers.

Under **Authentication Brokers**, you can also do the following:

- Add a new secondary Authentication Broker to the Veritas Operations Manager domain.
- Remove the secondary Authentication Broker from the Veritas Operations Manager domain.
- Refresh an Authentication Broker.

Under **Authentication Brokers**, you must select an Authentication Broker to view the domains that are associated with it. Under **Domains**, you can view the list of the authentication domains. You can view the following details for each authentication domain:

- **Domain Name**
- **Name of the authentication domain**
- **Domain Type**
- **Type of the authentication domain**
- **Status**
- **Displays whether the authentication domain is enabled or disabled**

Under **Domains**, you can do the following:

- Configure LDAP on an Authentication Broker.
Remove the LDAP configuration from an Authentication Broker.

Enable the authentication domain.

Disable the authentication domain.

To view the details of the Authentication Brokers and the domains associated with them,

2. Click Authentication Brokers.

See “About managing Authentication Brokers in the Veritas Operations Manager domain” on page 216.


See “Adding secondary Authentication Brokers to the Veritas Operations Manager domain” on page 219.

See “Refreshing the information associated with the Authentication Brokers” on page 222.

See “Removing the Authentication Brokers from the Veritas Operations Manager domain” on page 222.


See “Removing Lightweight Directory Access Protocol or Active Directory configuration from the primary Authentication Broker” on page 228.

See “Enabling the authentication domains associated with an Authentication Broker” on page 229.

See “Disabling the authentication domains associated with an Authentication Broker” on page 230.

---

**Adding secondary Authentication Brokers to the Veritas Operations Manager domain**

The **Add New Broker** wizard panel lets you add secondary Authentication Brokers to the Veritas Operations Manager domain. This task does not include installing Authentication Brokers. By default, in the **Security Settings** view, Veritas Operations Manager displays the primary Authentication Broker.

To use the user interface to add Authentication Brokers to the Veritas Operations Manager domain, you must use Symantec Product Authentication Service version...
6.0. If you use the Symantec Product Authentication Service version 4.3, you must use the command-line interface to add the secondary Authentication Brokers.

**Note:** Only the users with the Domain Admin role can manage Authentication Brokers.

### To add secondary Authentication Brokers

1. Select **Settings > Security**.

2. In the **Security Settings** view, under **Authentication Brokers**, click **Add**.

3. In the **Add New Broker** wizard panel, enter the details and click **OK**.

   See “**Add New Broker options**” on page 221.

4. In the **Results** panel that confirms that you added a secondary Authentication Broker to the Veritas Operations Manager domain, click **OK**.

### To add the secondary Authentication Brokers using the command-line interface

1. Add the Authentication Broker entry in the `broker_list.conf` file as follows:

   ```
   { "vxss://habas3th-03.vxindia.veritas.com:14545" : {
      "type":"primary", "domains" : [
         "habas3th-03.vxindia.veritas.com/unixpwd"
      ] },
   "vxss://habsolsprth-06.vxindia.veritas.com:2821" : {
      "type":"secondary", "domains" : [
         "habsolsprth-06.vxindia.veritas.com/unixpwd"
      ] }
   ```

   Depending on the platform of Management Server, you can locate the `broker_list.conf` file as follows:

   - Solaris and Red Hat Linux: `/etc/default/broker_list.conf`
   - Windows: `Drive name:\WINDOWS\system32\drivers\etc\broker_list.conf`

2. Depending on the platform of Management Server, set `EAT_HOME_DIR` as follows:

   - Solaris and Red Hat Linux: `EAT_HOME_DIR=/opt/VRTSsfmcs/sec`
   - Windows: `EAT_HOME_DIR=Drive name:\Program Files\VERITAS\VRTSsfmcs\sec`

3. Depending on the platform of Management Server, set `EAT_DATA_DIR` as follows:

   - Solaris and Red Hat Linux: `EAT_DATA_DIR=/var/opt/VRTSsfmcs/sec`
4 Execute the following command:

- Solaris and Red Hat Linux: `/opt/VRTSsfmh/bin/vssat setuptrust -b habsolsprth-06:2821 -s low`

- Windows: `Drive name:\Program Files\VERITAS\VRTSsfmcs\sec\bin\vssat setuptrust -b habsolsprth-06:2821 -s low`

5 Execute the following command to restart the Web GUI:

- Solaris and Red Hat Linux: `/opt/VRTSsfmcs/cweb/sfmw restart`

- Windows: Under Service Control Manager (services.msc), restart the Storage Manager Service service.

See “About managing Authentication Brokers in the Veritas Operations Manager domain” on page 216.

See “Viewing the details of the Authentication Brokers and the domains associated with them” on page 218.

See “Refreshing the information associated with the Authentication Brokers” on page 222.

Add New Broker options

Use this panel to enter the details of the secondary Authentication Broker that you want to add to the SF Manager domain.

Table 14-1 Add New Broker panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broker Hostname</td>
<td>Fully-qualified host name or IP Address of the Authentication Broker host that you want to add to SF Manager domain.</td>
</tr>
<tr>
<td>Port No</td>
<td>Port number on which the Authentication Broker is configured to run.</td>
</tr>
</tbody>
</table>

See “Adding secondary Authentication Brokers to the Veritas Operations Manager domain” on page 219.
Refresh the information associated with the Authentication Brokers

The Refresh Broker wizard panel lets you refresh an Veritas Operations Manager Authentication Broker so you can see the authentication domains that you have added to it.

After you refresh the Authentication Broker, you can go under Domains, and view the added authentication domains.

To refresh the information associated with an Authentication Broker

2. In the Security Settings view, under Authentication Brokers, select the Authentication Broker that you want to refresh.
4. In the Refresh Broker wizard panel, click Yes.
5. In the Results panel that confirms the refreshing of the Authentication Broker that you have selected, click OK.

See “About managing Authentication Brokers in the Veritas Operations Manager domain” on page 216.

See “Viewing the details of the Authentication Brokers and the domains associated with them” on page 218.

See “Adding secondary Authentication Brokers to the Veritas Operations Manager domain” on page 219.

Removing the Authentication Brokers from the Veritas Operations Manager domain

The Remove Broker wizard panel lets you remove secondary Authentication Brokers from the Veritas Operations Manager domain. When you remove an Authentication Broker, the operation does not uninstall the Authentication Broker. It only removes the Authentication Broker from the Veritas Operations Manager domain.

Note: You cannot remove the primary Authentication Broker from the Veritas Operations Manager domain.
To remove the secondary Authentication Brokers from the domain

1 Select Settings > Security.

2 In the Security Settings view, under Authentication Brokers, select the Authentication Broker that you want to remove.

3 Under Authentication Brokers click Remove Broker.

4 In the Remove Broker wizard panel to confirm whether you want to remove the Authentication Broker, click Yes.

5 In the Results panel that confirms that you removed the selected Authentication Brokers, click OK.

See “About managing Authentication Brokers in the Veritas Operations Manager domain” on page 216.

See “Viewing the details of the Authentication Brokers and the domains associated with them” on page 218.

Configuring Lightweight Directory Access Protocol-based authentication on the Management Server host

You can configure Lightweight Directory Access Protocol (LDAP)-based authentication on the primary authentication broker.

Note: By default, the LDAP-based authentication domain that you configure is in the enabled state.

To configure LDAP-based authentication

1 Select Settings > Security.

2 In the Security Settings view, under Domains, click Configure LDAP/AD.

3 In the LDAP/AD Settings - discover attributes and configuration information wizard panel, enter the details and click Next.

See “LDAP/AD Settings - discover attributes and configuration information panel options” on page 224.
4 In the **LDAP/AD Settings - configure LDAP/AD** wizard panel, specify the search base and click **Finish**.

See “**LDAP/AD Settings - configure LDAP based authentication options**” on page 226.

5 In the **Results** panel that confirms that you have configured LDAP based authentication, click **OK**.

See “**About managing domains associated with an Authentication Broker in Veritas Operations Manager**” on page 217.

See “**Viewing the details of the Authentication Brokers and the domains associated with them**” on page 218.

See “**Removing Lightweight Directory Access Protocol or Active Directory configuration from the primary Authentication Broker**” on page 228.

See “**Enabling the authentication domains associated with an Authentication Broker**” on page 229.

See “**Disabling the authentication domains associated with an Authentication Broker**” on page 230.

See “**Adding security groups to the Veritas Operations Manager domain**” on page 182.

---

**LDAP/AD Settings - discover attributes and configuration information panel options**

Use this wizard panel to start configuring Lightweight Directory Access Protocol (LDAP) based authentication on the primary authentication broker.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Information</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Server Name (Mandatory)** | Fully-qualified host name or IP address of the LDAP server.  
If a secure session is configured with the LDAP server using SSL certificates, you must enter the fully-qualified hostname that matches with the fully-qualified hostname in the LDAP server certificate. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong> (Mandatory)</td>
<td>Number of the port on which the LDAP server is configured to run. By default, this field displays the port number as 389. You can edit this port number, if required.</td>
</tr>
<tr>
<td><strong>This server requires me to log on</strong> (Optional)</td>
<td>Check this check box if the anonymous operations are disabled on the LDAP server and a bind user ID is required to proceed with configuring the LDAP-based authentication.</td>
</tr>
<tr>
<td><strong>Bind User Name/DN</strong></td>
<td>The complete Distinguished Name (DN) of the user that is used to bind to the LDAP server. If the LDAP server being used is Active Directory (AD), you can provide the DN in any of the following formats:</td>
</tr>
<tr>
<td></td>
<td>■ <a href="mailto:username@domainname.com">username@domainname.com</a></td>
</tr>
<tr>
<td></td>
<td>■ domainname\username</td>
</tr>
<tr>
<td></td>
<td>For example, You can provide the DN as <a href="mailto:Administrator@enterprise.domainname.com">Administrator@enterprise.domainname.com</a> ENTERPRISE\Administrator For RFC 2307 compliant LDAP servers, specify complete bind DN. For example, cn=Manager,dc=vss,dc=symantec,dc=com The LDAP or the AD administrator can provide you the bind user name that you can use.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password that is assigned to the bind user name that you use.</td>
</tr>
<tr>
<td><strong>Use Secure Sockets Layer</strong></td>
<td>Check this checkbox to use the Secure Sockets Layer (SSL) certificates to establish a secure channel between the authentication broker and the LDAP server.</td>
</tr>
</tbody>
</table>
Table 14-2  LDAP/AD Settings - discover attributes and configuration information panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate location</td>
<td>Location of the trusted root CA certificate of the vendor that issued the LDAP server certificate.</td>
</tr>
</tbody>
</table>

Query Information

<table>
<thead>
<tr>
<th>User Name (Mandatory)</th>
<th>User name that the system use to detect the LDAP server-related settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: You must ensure that the user name that you enter does not contain any special characters. For example, you must not enter the special character ‘(‘ in this field.</td>
<td></td>
</tr>
<tr>
<td>The system determines the search base based on the user name that you specify in this field.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Name of the user group that the system use to detect the LDAP server-related settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: Make sure that the group name that you enter does not contain any special characters. For example, you must not enter the special character ‘(‘ in this field.</td>
<td></td>
</tr>
<tr>
<td>The system determines the search base based on the group name along with the user name that you have specified.</td>
<td></td>
</tr>
</tbody>
</table>


LDAP/AD Settings - configure LDAP based authentication options

Use this wizard panel to specify the Domain Name and the Search Base to configure Lightweight Directory Access Protocol (LDAP) based authentication on the primary authentication broker.
## Table 14-3  LDAP/AD Settings - configure LDAP based authentication options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name</strong></td>
<td>Displays the fully-qualified host name or IP Address of the LDAP server that you have specified in the <strong>LDAP/AD Settings - discover attributes and configuration information</strong> wizard panel. You cannot edit this field.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>Unique name to identify the LDAP based authentication that you configure on the primary authentication broker. <strong>Note:</strong> In the <strong>Domain Name</strong> field, you can enter up to 32 characters.</td>
</tr>
<tr>
<td><strong>Search Base</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Use Default</strong></td>
<td>Select this option if you want to use the default search base that the system has detected using the information that you have specified on the <strong>LDAP/AD Settings - discover attributes and configuration information</strong> wizard panel.</td>
</tr>
</tbody>
</table>
Table 14-3  LDAP/AD Settings - configure LDAP based authentication options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Custom | Select this option to specify the search base other than the default search base.  
For example, you can customize the search base as follows to authenticate the user (sampleuser) who belongs to the organization (ou=HR), which is an organization unit under ou=user:  
The organization structure is given below:  
ou=HR,ou=People,dc=veritas,dc=com  
|--sampleuser  
ou=Engg,ou=People,dc=veritas,dc=com  
|--Eng1  
The default search base is  
ou=HR,ou=People,dc=veritas,dc=com  
To authenticate users under ou=HR and ou=Engg, set custom search base to a level up:  
ou=People,dc=symantec,dc=com |


Removing Lightweight Directory Access Protocol or Active Directory configuration from the primary Authentication Broker

The Unconfigure LDAP wizard panel lets you remove Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) configuration from the primary Authentication Broker.

To remove LDAP or AD configuration from the primary Authentication Broker

1. Select **Settings > Security**.
2. In the **Security Settings** view, under **Domains**, select the authentication domain that you have configured as LDAP or AD.
3 Under **Domains**, click **Unconfigure LDAP**.

4 In the **Results** panel that confirms that you removed the authentication domain that is configured as LDAP or AD, click **OK**.

See “About managing Authentication Brokers in the Veritas Operations Manager domain” on page 216.

See “Viewing the details of the Authentication Brokers and the domains associated with them” on page 218.


---

### Enabling the authentication domains associated with an Authentication Broker

The **Enable Domain** wizard panel lets you enable one or more authentication domains.

You must enable an authentication domain to do the following:

- Display the authentication domain on the Veritas Operations Manager Login page.
- Add the authentication domain to a security group.

**To enable the authentication domains associated with an Authentication Broker**

1 Select **Settings > Security**.

2 In the **Security Settings** view, under **Domains**, select one or more authentication domains that you want to enable.

3 Under **Domains**, click **Enable Domains**.

4 In the **Enable Domain** wizard panel, enter the details and click **OK**.

See “Enable Domains options” on page 230.

5 In the **Results** panel that confirms that you enabled the selected authentication domains, click **OK**.


See “Viewing the details of the Authentication Brokers and the domains associated with them” on page 218.

Enable Domains options

Use this panel to enable the Authentication Broker that you have selected.

Table 14-4 Enable Domains panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Name of the Authentication Domain that you have selected to enable.</td>
</tr>
<tr>
<td>Domain Type</td>
<td>Type of the Authentication Domain that you have selected to enable.</td>
</tr>
</tbody>
</table>

Disabling the authentication domains associated with an Authentication Broker

The Disable Domain wizard panel lets you disable one or more authentication domains.

To disable the authentication domains associated with an Authentication Broker

1 Select Settings > Security.
2 In the Security Settings view, under Domains, select one or more authentication domains that you want to disable.
3 Under Domains, click Disable Domains.
4 In the Disable Domains wizard panel, review the details and click OK.
5 In the Results panel that confirms that you disabled the selected authentication domains, click OK.


See “Viewing the details of the Authentication Brokers and the domains associated with them” on page 218.

See “Enabling the authentication domains associated with an Authentication Broker” on page 229.

Disable Domains options

Use this panel to disable the Authentication Domain that you have selected.

Table 14-5 Disable Domains panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Name of the Authentication Domain that you have selected to disable.</td>
</tr>
<tr>
<td>Domain Type</td>
<td>Type of the Authentication Domain that you have selected to disable.</td>
</tr>
</tbody>
</table>

See “Disabling the authentication domains associated with an Authentication Broker” on page 230.
Disabling the authentication domains associated with an Authentication Broker
Managing licenses in Veritas Operations Manager

This chapter includes the following topics:

- About License Deployment Report
- Advantages of using License Deployment Report
- About Symantec Licensing and Pricing
- About assigning price tiers to hosts
- About uploading price tier information
- About license deployment policies
- Viewing platform specific licensing and pricing information
- Assigning a price tier to a host
- Uploading the Price Tier file to Management Server
- Viewing the details of license deployment policies
- Creating a license deployment policy
- Modifying a license deployment policy
- Updating the default virtual machine count factor in Veritas Operations Manager
- Removing a license deployment policy
About License Deployment Report

License Deployment Report (LDR) helps customers by leveraging Storage Foundation Manager infrastructure to generate report on deployed product licenses according to their respective price tiers. The LDR reduces reconciliation time and may lead to have less customer and sales executive engagement. The LDR highlights hosts which have demo, evaluation, expired, verification needed license keys. It helps you to identify the wastage of licenses and usage of proper license keys according to product.

The License Deployment Report enables you to obtain and view information about Storage Foundation product licenses. This information about Storage Foundation product licenses is available in the deployment report.

The deployment report gives the following details:

- Tiering Information, that is, Server, Processor, NProcessors and OS price tiers.
- Product inventory for each host.
- Features enabled for each particular license key.
- Feature Evidence along with marker files and number of objects.

The License Deployment Report (LDR) identifies price tiers, make or model of hosts, number of processors, installed OS and so on. It also identifies Symantec price tier such as Server price tier, Processor price tier, NProcessor price tier, and Installed OS price tier. In addition to this it identifies list of hosts for assigning price tier, and each unquie product. In LDR, you can assign price tiers to the hosts depending on the requirement and configuration. You can use OS-specific commands to view the characteristics of hosts such as the model, the host make, the processor type, and the processor count. ou can use the LDR to highlight deployed products. The identifies number of hosts, and number of deployed licenses. You can view deployment summary charts such as

License Deployment Report enables you to review deployment summary charts where the summary is shown as percentages using the following bar charts:

- Summary by product.
- Summary by platforms.
- Summary by edition.
- Summary by release.

License Deployment Report provides the real time status of the licences deployed on the manged hots that are added to Management Server. License Deployment Report automatically discovers the licenses that are deployed on a managed host when it is added to Management Server. The results are displayed in the Licenses
view. By default, License Deployment Report discovers the licences deployed on
the managed hosts in an interval of two hours.

If you want to identify the status of the Storage Foundation licenses in a datacenter,
each individual server must be manually examined. This process can take much
time and effort, because a datacenter may have many types of hosts, and each
host can have a variety of software installed on it. The hosts for which you are
not able to find details of characteristics of hosts such as the model, the host make,
the processor type, and the processor count are termed as "unknown hosts". In
LDR, you can assign price tiers to the hosts depending on the requirement and
configuration.

The latest price tier information is available with the License Deployment Report.
You can perform the Upload Price Tier File operation to upload new price tier
information to Management Server.

You can use the **Product Inventory** tab to view the types of products, the platforms
they are running on, their editions, their release version, the price tier to which
they belong, and so on. You can also click the link under the Inventory tab to sort
the view which is grouped according to All, Edition), Release, and Platform. You
can use the product inventory view to view host level and product level deployment
issues.

You can use the **Product-Tier Mapping** tab to view the following:

- **Deployments by Server Price Tier**
  Displays the Server Price Tier information that is categorized using the
  alphabets A to N.

- **Deployments by Processor Type Price Tier**
  Displays the information on processor type price tier.

- **Deployments by NProcessors Price Tier**
  The information in Deployments by NProcessors Price Tier represents pricing
  per Number of Processors.

- **Deployments by Installed OS Price Tier**
  The information in Deployments by Installed OS Price Tier represents pricing
  per Installed OS.

You can use **Tier-Host Mapping** tab lets you find the match type for each host. It
displays the matrix for each Price Tier, such as the number of exact matches,
number of best matches, and the number of times the users defined the match.

The **Exceptions** tab displays the list of hosts that are not considered in counting
the license deployments.

The exception can be because of any of the following:

- Licenses for Storage Foundation and Storage Foundation-HA are not found.
Advantages of using License Deployment Report

Typically, if you want to check the status of your Storage Foundation licenses, you must examine each server individually. Because a data center may have many types of hosts running a variety of software, this can be a time-consuming process.

The Storage Foundation License Deployment Reporter (LDR) lets you gather Storage Foundation license key and deployment information from a single location. The LDR generates accurate reports about the hosts running Storage Foundation products.

License Deployment Report has the following benefits:

- License deployment discovery that is failed to run.
- License deployment discovery is in progress.

License Deployment Report discovers the keyless licenses along with the traditional license keys. The keyless licenses are not reported in the columns that displays the Verification needed or the Over deployed information.

The License Deployment Report provides information about product name, product version, edition, tier, and quantity in tabular format. In addition to this it also gives detailed information about the tiering information, that is, price tier and processor tier. The deployment report also gives a detailed product inventory for each host, and features enabled for each particular license key. You can use the Product Evidence feature to installed product bits, version of installed product, and features evidence along with the marker files and number of objects.

See “About Symantec Licensing and Pricing” on page 237.
See “About License Deployment Summary view” on page 258.
See “About assigning price tiers to hosts” on page 240.
See “About uploading price tier information” on page 240.
See “Viewing platform specific licensing and pricing information” on page 241.
See “Viewing the summary of product inventory” on page 267.
See “Viewing the Tier-Host Mapping summary” on page 271.
See “Viewing product details by host name” on page 272.
See “Viewing product details by license key” on page 279.
See “Viewing License Key details” on page 281.
See “Viewing the overview of a host” on page 275.
Generates a deployment report about the product, product version, and product release.

Reduces the time that sales engineers and customers need to physically inventory the installed base.

Provides the customer with information about deployment, which is needed for license renewal.

Reduces the time needed to renew licenses.

About Symantec Licensing and Pricing

The Storage and Server Management, High Availability products which operate on UNIX (Solaris, HP-UX, and AIX), Linux and Windows must be certified to work on servers. This product certification differs from platform to platform. Certification is how Storage and Server Management, High Availability products are licensed by platform. Symantec refers to licenses as price tier information. Price tier information is provided in an Excel document when the LDR is installed. The document contains information about all the product and platforms.

The Symantec licenses and price tiers are based on the following:

- **UNIX Pricing Tier (AIX, HP-UX, and Solaris)**
  - The Veritas Storage and Server Management, High Availability products on UNIX (Solaris, HP-UX, and AIX) are generally licensed and priced on a per-tiered-server meter, regardless of the number of domains on the server. Licenses for Storage Foundation and HA products for UNIX platforms can be licensed in any of the following ways:
    - **Per Tiered Server Meter/Pricing**
      - The Veritas Storage and Server Management, High Availability products on UNIX are generally licensed and priced per server. The pricing depends on the server price tier to which a server is assigned. A server can be assigned to 14 different server tiers from Tier A through Tier N. Customers must pay the per-server price for each server that runs Storage and Server Management, High Availability products. This pricing meter applies to all versions of Veritas Storage and Server Management, High Availability products on UNIX (Solaris, HP-UX, and AIX).
    - **Per Tiered Processor Meter/Pricing (UxRT 5.x only)**
      - Starting with UxRT 5.0, the Veritas Storage and Server Management, High Availability products on UNIX can be licensed and priced per tiered Processor. The price depends on the processor price tier to which a processor is assigned. A processor can be assigned to three different processor tiers from Processor Tier 1 through Processor Tier 3. Customers
must pay the per-tiered-processor price for every processor that runs Storage and Server Management, High Availability products.

- **Linux Pricing Tier (Red Hat and Novell SUSE)**
The Veritas Storage and Server Automation, High Availability for Linux is licensed on a per-processor basis regardless of the number of cores on the processor. As such, a multicore chip with “n” cores counts as one processor. For example, each dual-core AMD Opteron processor that runs Storage Foundation for Linux requires one processor license.

- **Windows Pricing Tier**
The Veritas Storage and Server Automation, High Availability products which operate on the Microsoft Windows operating system are priced per server. The price also depends on the edition of Windows that is installed; for example, NT or 2000. The Storage Foundation and High Availability products on Windows do not follow a per-processor pricing meter.

<table>
<thead>
<tr>
<th>Table 15-1 Symantec price tiers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Price tier</strong></td>
</tr>
<tr>
<td>A, B, C, D, E, F, G, H, I, J, K, L, M, N</td>
</tr>
</tbody>
</table>
### Table 15-1  Symantec price tiers (continued)

<table>
<thead>
<tr>
<th>Price tier</th>
<th>Tier type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1, Tier 2, Tier 3</td>
<td>Processor type</td>
<td>Starting with UxRT 5.0, Veritas Storage and Server Management, High Availability products on UNIX can be licensed and priced per tiered processor. The per-tiered-processor price depends on the processor price tier that a processor is assigned to. A processor can be assigned to one of three processor tiers (Processor Tier 1, 2, or 3). You must pay the per-tiered-processor price for every active processor running Storage and Server Management, High Availability products.</td>
</tr>
<tr>
<td>1, 2, 3, 4, 5, 6, 7, 8 Processors</td>
<td>NProcessors</td>
<td>The Veritas Storage and Server Automation, High Availability products for Linux are licensed on a per-processor basis regardless of the number of cores on the processor. A multicore chip with “n” cores counts as one processor. For example, each dual-core AMD Opteron processor that runs Storage Foundation for Linux requires one processor license.</td>
</tr>
</tbody>
</table>
Table 15-1  Symantec price tiers (continued)

<table>
<thead>
<tr>
<th>Price tier</th>
<th>Tier type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1, Level 2, Level 3,</td>
<td>Installed operating system</td>
<td>The Veritas Storage and Server Automation, High Availability products which operate on the Microsoft Windows operating system are priced per server. The price depends on the particular edition of that is installed, for example, Windows NT or 2000, not according to the processor capacity of the server.</td>
</tr>
</tbody>
</table>

See “Viewing platform specific licensing and pricing information” on page 241.

About assigning price tiers to hosts

You can use operating system-specific commands to find host characteristics, including the model, make, processor type, and processor count. However, although you can discover hardware information for most hosts, you may not have all the characteristics of a host. In that case, it is called an "unknown tier."

The assign price tier feature lets you assign price tiers to an unknown host. It eliminates the need to find host characteristics manually.

You can assign a price tier to a host by selecting the server price tier, processor type price tier, or processors price tier according to the characteristics of the host, such as the make, model, processor type, number of processors, and operating system.

See “About License Deployment Report” on page 234.
See “Assigning a price tier to a host” on page 243.

About uploading price tier information

Price tier information is available with License Deployment Report. You can perform the Upload Price Tier File operation to upload new price tier information to Management Server. You must upload new price tier in a comma separated values (.csv) file.
The Storage Foundation Manager 1.1 Management Server does not contain information about platform price tier mapping. You should upload this information in a comma separated values (.csv) file to the management server during installation. If you do not upload price tier information during installation, you can upload it from the License Deployment Reporter Tasks view.

The changes in price tier are valid to you when you upload the new price tier file. The earlier version of the price tier file is not replaced. Instead, the management server derives price tier information from both the earlier version and the latest version of the file.

For example, suppose Server A belongs to Tier 1 in one version of the price tier file. After Symantec changes the price tier, the new price tier file has Server A priced as Tier 2. In this case, the Symantec Licensing office does not change the existing price tier of Server A, despite the update. However, if you deploy a new Server A, the new price tier charge would be in effect.

See “About License Deployment Report” on page 234.

See “Uploading the Price Tier file to Management Server” on page 245.

About license deployment policies

Veritas Operations Manager lets you create license deployment policies to manage the license deployment in the datacenter.

You can define a low watermark and a high watermark for a specific license. If the number of licenses that you have deployed in the datacenter exceed the low watermark value, Veritas Operations Manager generates a warning. If the number of licenses that you have deployed exceed the high watermark value, Veritas Operations Manager generates an alert. Veritas Operations Manager displays this alert in the Alerts view.

Viewing platform specific licensing and pricing information

Veritas Storage and Server Management, High Availability products on UNIX (Solaris, HP-UX, and AIX) are typically licensed and priced on a per-tiered-server meter, regardless of the number of domains on the server. Starting with UxRT 5.0, UxRT products are sold on a per-tiered-server pricing meter or a per-tiered-processor pricing meter.

Licenses for UNIX products are priced in the following ways:

- Per tiered server meter/pricing
Veritas Storage and Server Management, High Availability products on UNIX are generally licensed and priced per server. The per-server price depends on the server price tier that a server is assigned to. A server can be assigned to one of 13 server tiers (Tier 1A through Tier 4D). You must pay the per-server price for each server running Storage and Server Management, High Availability products. This pricing meter applies to all versions of Veritas Storage and Server Management, High Availability products on UNIX (Solaris, HP-UX, and AIX).

■ Per tiered processor meter/pricing (UxRT 5.x only)
Starting with UxRT 5.0, Veritas Storage and Server Management, High Availability products on UNIX can be licensed and priced per tiered processor. The per-tiered-processor price depends on the processor price tier that a processor is assigned to. A processor can be assigned to one of three processor tiers (Processor Tier 1, 2, or 3). You must pay the per-tiered-processor price for every active processor running Storage and Server Management, High Availability products.

**Note:** Storage and Server Automation, High Availability for Linux is licensed on a per-processor basis, regardless of the number of cores on the processor. A multicore chip is considered one processor. For example, each dual-core AMD Opteron processor running Storage Foundation for Linux requires one processor license.

**Note:** Storage and Server Automation, High Availability products running on the Microsoft Windows operating system are priced per server, according to the Windows edition that is installed, for example, Windows NT or Windows 2000. The pricing is not based on the server's processor capacity.

**To view platform specific licensing and pricing information**
1. In the Veritas Operations Manager console, select **Licenses > Tier Information**.
2. To view licensing and pricing information specific to a platform, click one of the following tabs:
   - Solaris
   - HP-UX
   - AIX
   - Linux
   - Windows
Assigning a price tier to a host

The characteristics of a host determine its price tier. These characteristics include the make, model, processor type and number, and operating system.

To assign a price tier to a host

1. In the Veritas Operations Manager console, select Licenses > Deployment Summary.

2. In the Deployment Summary view, under Deployed Host Summary, click the number that represents the Number of Hosts category.

3. In the Hosts having license deployed view, check the check box for the host to which you want to assign the price tier and click Assign Price Tier.

4. In the Select Price Tier panel, specify the appropriate information and click Next.

   See “Select Price Tier options” on page 243.

5. If you want to assign the price tier to other hosts with similar configuration, specify those hosts in the Hosts having similar configuration panel and click Next.

   See “Select hosts to set chosen tier options” on page 245.

6. In the Assign price tier summary panel, view the summary of the price tier and the hosts that you have selected and click Finish.

   See “Assign price tier summary” on page 245.

7. In the Results panel that confirms the action, click OK.

   See “About License Deployment Report” on page 234.

   See “About assigning price tiers to hosts” on page 240.

   See “About the product inventory summary” on page 259.

Select Price Tier options

Use this wizard panel to assign the latest price tier to the host on which the licenses are deployed.
Note: All the information may not apply for a host that you have selected. You can specify the values from the drop-down boxes for the information that are applicable for the host.

Table 15-2  Select Price Tier panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Server Price Tier</td>
<td>Select the appropriate Server price tier. Server price tiers are represented using alphabets A through N. Server price tier applies to Solaris, HP-UX, and AIX platforms.</td>
</tr>
<tr>
<td>Select Processor Type Price Tier</td>
<td>Select the appropriate Processor price tier. Processor type price tiers are represented as Tier 1, Tier 2, Tier 3, and Tier 4. Processor price tier applies to all supported platforms.</td>
</tr>
<tr>
<td>Select NProcessors Price Tier</td>
<td>Select the appropriate NProcessors price tier. NProcessor price tiers are represented using integers 1 through 8. NProcessor price tier applies to the Linux platform.</td>
</tr>
<tr>
<td>Select OS Price Tier</td>
<td>Select the appropriate OS price tier. OS price tiers are represented as Level 1, Level 2, and Level 3. OS price tier applies to Windows and virtual Windows platforms.</td>
</tr>
<tr>
<td>Do you want to set tier to other hosts having same configuration?</td>
<td>Select this check box if you want to assign the price tier to other hosts with similar configuration integers. This check box is enabled only if you have multiple hosts that have similar configuration. The Select hosts to set chosen tier panel is displayed only if you select this check box.</td>
</tr>
</tbody>
</table>

See “Assigning a price tier to a host” on page 243.
Select hosts to set chosen tier options

Use this panel to select one or more hosts with similar configuration on which you want to assign the price tier.

This panel is displayed only if you have selected the **Do you want to set tier to other hosts having same configuration?** check box in the **Select Price Tier** panel.

See “Assigning a price tier to a host” on page 243.

Assign price tier summary

Use this panel to view the list of host to which the selected price tier is assigned.

See “Assigning a price tier to a host” on page 243.

Uploading the Price Tier file to Management Server

The Symantec Licensing Office provides you with the Price Tier information in a comma-separated values (.csv) file. You are provided with the location of the file which has to be uploaded to Management Server.

You can navigate to the **Monitoring > Tasks** to view the status of the Price Tier upload task.

**To upload Price Tier information**

1. Select **Licensing > Tier Information**.
2. On the left side panel, click **Upload Price Tier File** link.
3. In the **Upload Price Tier File wizard** panel, select the Price Tier file to be uploaded to Management Server and click **Upload**.

See “Upload Price Tier File options” on page 245.

4. Click **Finish** to complete the task.

See “About License Deployment Report” on page 234.

See “About uploading price tier information” on page 240.

See “About Symantec Licensing and Pricing” on page 237.

Upload Price Tier File options

Use this wizard panel to select the **PriceTier.csv** file from a specified location and upload it to Management Server.

Also, this panel displays the following information:
Current version of the PriceTier.csv file available in the datacenter.

The location from where you can download the latest PriceTier.csv file.

See “Uploading the Price Tier file to Management Server” on page 245.

Viewing the details of license deployment policies

License deployment policies view lists all the license deployment policies that you have created in Veritas Operations Manager. The details of the license deployment policies are displayed in a table. Each row in the table represents a license deployment policy. The license deployment policy for which the licenses have exceeded the higher threshold value is highlighted in red. The row that represents the license deployment policy for which the licenses have exceeded the lower threshold value is highlighted in yellow.

In this view, you can perform the following operations:

- Create the license deployment policy.
- Change thresholds for license deployment policy
- Remove the license deployment policy.

The left-side panel provides you the options to filter the license deployment policies that are displayed on this table. You can enter the policy name or the product name in the Search text box at the top of the left-side panel to sort the License deployment policies table.

Review the following information on this page:

- Name: Name of the license deployment policy.
- Business entity: The name of the applied business entity to the deployment policy. It is displayed only when you have applied a business entity to the deployment policy when you created the deployment policy.
- Platform: The platform based on which the licenses are deployed.
- Virtual machine: Indicates whether the deployment policy is applied for a virtual machine.
- Product: The Storage Foundation product for which you have created the deployment policy.
- Product Edition: The edition of the Storage Foundation product for which you have created the deployment policy.
- Version: The version of the Storage Foundation product for which you have created the deployment policy.
- Tier Type: The tier type for the deployment policy. For example, PROCESSOR and server.
- Tier: The tier value for the deployment policy.
- Lower threshold: The set lower threshold value for the deployment policy.
- Higher threshold: The set higher threshold value for the deployment policy.
- #Deployments: The policy deployment count.

Also, the left-side panel displays the following categories that lets you filter the License deployment policy table:

- Platform
- Virtual machine
- Violation Type
- Edition
- Version

Under each category, you can use the options to filter the table.

**To view the details of license deployment policies**

1. In the Veritas Operations Manager console, select **Licenses > Deployment Policy**.
2. In the **License deployment policies** table, review the details of the license deployment policies.

   See “License deployment policies table details” on page 247.

See “Creating a license deployment policy” on page 248.

See “Removing a license deployment policy” on page 255.

See “Modifying a license deployment policy” on page 251.

**License deployment policies table details**

Table 15-3 table explains the information that is displayed in the License deployment policies table.

**Table 15-3** Details of the License deployment policies

<table>
<thead>
<tr>
<th>Name of column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Platform based on which the licenses are deployed.</td>
</tr>
</tbody>
</table>
Table 15-3  Details of the License deployment policies (continued)

<table>
<thead>
<tr>
<th>Name of column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Storage Foundation product for which you want to create a deployment policy.</td>
</tr>
<tr>
<td>Edition</td>
<td>Edition of the product for which you want to create the deployment policy.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the product for which you want to create the deployment policy.</td>
</tr>
<tr>
<td>Tier Type</td>
<td>Tier types based on the platform on which the licenses are deployed</td>
</tr>
<tr>
<td>Tier</td>
<td>Price Tier based on the platform that you choose to create the license deployment policy.</td>
</tr>
<tr>
<td>Lower threshold</td>
<td>Number of license deployments for which Veritas Operations Manager must generate a warning.</td>
</tr>
<tr>
<td>Higher threshold</td>
<td>Number of license deployments for which Veritas Operations Manager must generate an alert.</td>
</tr>
<tr>
<td>#Deployments</td>
<td>Number of the licenses that are deployed in the datacenter.</td>
</tr>
</tbody>
</table>

Creating a license deployment policy

You can create a license deployment policy to manage the deployment of licenses in the datacenter.

Create a license deployment policy

1  In the Veritas Operations Manager console, select Licenses > Deployment Policy.
2  In the License deployment policies view, click Create Policy.
3  In the Create/Modify license deployment policy wizard panel, enter the details and click Next.

See “Create license deployment policy options” on page 249.
4 In the **Deployment Policy Summary** wizard panel, view the summary of the details that you have entered and click **Finish**.

See “**Deployment Policy Summary**” on page 251.

5 In the **Results** panel that confirms the creation of the deployment policy, click **OK**.

See “**Modifying a license deployment policy**” on page 251.

See “**Removing a license deployment policy**” on page 255.

---

**Create license deployment policy options**

Use this wizard panel to create a license deployment policy.

**Table 15-4** Create license deployment policy panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Specify the name of the deployment policy. You can use the name to identify the deployment policy later. For example, the name of the policy helps you identify the policy in an alert message. <strong>Note:</strong> In Veritas Operations Manager 3.1, you can identify the policies using the policy names. The policies that were created using the earlier versions of Veritas Operations Manager does not contain policy name. However, you can add names to such policies when you modify them using the Change Threshold wizard panel. You can only change the lower and the higher threshold values for a policy that has a policy name.</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Choose the platform based on which the licenses are deployed.</td>
</tr>
<tr>
<td><strong>Virtual machine</strong></td>
<td>Check this check box if you want to apply the deployment policy that you create for the virtual machine.</td>
</tr>
</tbody>
</table>
Table 15-4  Create license deployment policy panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier Type</td>
<td>Choose one of the following price tier types based on the platform on which the licenses are deployed:</td>
</tr>
<tr>
<td></td>
<td>■ Server</td>
</tr>
<tr>
<td></td>
<td>■ Processor</td>
</tr>
<tr>
<td></td>
<td>■ NProcessors</td>
</tr>
<tr>
<td></td>
<td>■ OS</td>
</tr>
<tr>
<td></td>
<td>Here is the list of platforms and their tier types:</td>
</tr>
<tr>
<td></td>
<td>■ Linux - Processor and NProcessor price tiers</td>
</tr>
<tr>
<td></td>
<td>■ Solaris, HP-UX, and AIX - Server and Processor price tiers</td>
</tr>
<tr>
<td></td>
<td>■ Virtual Linux, Solaris, HP-UX, and AIX - Processor price tier</td>
</tr>
<tr>
<td></td>
<td>■ Windows and virtual Windows - Processor and OS price tiers</td>
</tr>
<tr>
<td>Price Tier</td>
<td>Choose the price tier based on the platform that you choose.</td>
</tr>
<tr>
<td></td>
<td>The following list explains the tier types and the price tiers for them:</td>
</tr>
<tr>
<td></td>
<td>■ Processor tier - Tier 1, Tier 2, Tier 3, and Tier 4.</td>
</tr>
<tr>
<td></td>
<td>■ NProcessor tier - Integers 1-8.</td>
</tr>
<tr>
<td></td>
<td>■ Server tier - Alphabets A-N.</td>
</tr>
<tr>
<td></td>
<td>■ OS tier - Level 1, Level 2, and Level 3.</td>
</tr>
<tr>
<td>Product</td>
<td>The Storage Foundation product for which you want to create a deployment policy.</td>
</tr>
<tr>
<td></td>
<td>If you choose the Windows platform, you can choose any of the following products:</td>
</tr>
<tr>
<td></td>
<td>■ Storage Foundation for Windows</td>
</tr>
<tr>
<td></td>
<td>■ Storage Foundation HA for Windows</td>
</tr>
<tr>
<td></td>
<td>■ Storage Foundation HA/DR for Windows</td>
</tr>
<tr>
<td>Product Edition</td>
<td>Choose the edition of the product for which you want to create the deployment policy.</td>
</tr>
</tbody>
</table>
Table 15-4 Create license deployment policy panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Choose the version of the product for which you want to create the deployment policy.</td>
</tr>
<tr>
<td>Lower threshold</td>
<td>Enter the number of license deployments for which Veritas Operations Manager must generate a warning.</td>
</tr>
<tr>
<td>Higher threshold</td>
<td>Enter the number of license deployments for which Veritas Operations Manager must generate an alert. You must verify the license deployments in your datacenter.</td>
</tr>
<tr>
<td>Do you wish you apply Business Entity to the policy?</td>
<td>Select this check box if you want to associate one or more business entities with the policy.</td>
</tr>
</tbody>
</table>

See “Creating a license deployment policy” on page 248.

Deployment Policy Summary

Use this panel to view the details of the information that you have provided in the Create license deployment policy options panel.

See “Creating a license deployment policy” on page 248.

Modifying a license deployment policy

You can modify the low watermark and high watermark values for a license deployment policy that you have created.

**Note:** In Veritas Operations Manager 3.1, you can identify the policies using the policy names. The policies that were created using the earlier versions of Veritas Operations Manager does not contain policy name. However, you can add names to such policies when you modify them using the Change Threshold wizard panel. You can only change the lower and the higher threshold values for a policy that has a policy name.
To modify a license deployment policy

1. In the Veritas Operations Manager console, select **Licenses > Deployment Policy**.

2. In the **License deployment policies** view, check the check box for the deployment policy that you want to modify and click **Edit Policy**.

3. In the **Create/Modify license deployment policy** wizard panel, modify the values in the **Low threshold** and **Higher threshold** fields as required and click **Next**.

   See “**Change thresholds of license deployment policy options**” on page 252.

4. In the **Deployment Policy Summary** wizard panel, view the summary of the details that you have entered and click **Finish**.

   See “**Deployment Policy Summary (modify) options**” on page 254.

5. In the **Results** panel that confirms the creation of the deployment policy, click **OK**.

   See “**Creating a license deployment policy**” on page 248.

   See “**Removing a license deployment policy**” on page 255.

**Change thresholds of license deployment policy options**

Use this wizard panel to modify the **Lower threshold** and the **Higher threshold** values that you have defined for a license deployment policy.

If the policy that you want to edit has no name, you can provide a name to the policy in this panel.
Table 15-5  Change thresholds of license deployment policy panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the policy that you have provided.</td>
</tr>
<tr>
<td></td>
<td>If the policy that you want to edit has no name, you can provide a name to the policy in this field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In Veritas Operations Manager 3.1, you can identify the policies using the policy names. The policies that were created using the earlier versions of Veritas Operations Manager does not contain policy name. However, you can add names to such policies when you modify them using the Change Threshold wizard panel. You can only change the lower and the higher threshold values for a policy that has a policy name.</td>
</tr>
<tr>
<td>Platform</td>
<td>Displays the platform that you chose when you create the license deployment policy. You cannot edit this field.</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>Displays the selection that you have made when you create the license deployment policy. You cannot edit this field.</td>
</tr>
<tr>
<td>Tier Type</td>
<td>Displays the tier type that you chose when you create the license deployment policy. You cannot edit this field.</td>
</tr>
<tr>
<td>Price Tier</td>
<td>Displays the Price Tier that you chose when you create the license deployment policy. You cannot edit this field.</td>
</tr>
<tr>
<td>Product</td>
<td>Displays the Storage Foundation product that you chose when you create the license deployment policy. You cannot edit this field.</td>
</tr>
<tr>
<td>Product Edition</td>
<td>Displays the edition of the Storage Foundation product that you chose when you create the license deployment policy. You cannot edit this field.</td>
</tr>
</tbody>
</table>
Table 15-5  Change thresholds of license deployment policy panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Displays the version of the Storage Foundation product that you chose when you create the license deployment policy. You cannot edit this field.</td>
</tr>
<tr>
<td>Lower threshold</td>
<td>Modify the number of license deployments for which Veritas Operations Manager must generate a warning.</td>
</tr>
<tr>
<td>Higher threshold</td>
<td>Modify the number of license deployments for which Veritas Operations Manager must generate an alert. You must verify the license deployments in your datacenter.</td>
</tr>
<tr>
<td>Business Entity</td>
<td>Displays the business entities that are associated with the policy.</td>
</tr>
</tbody>
</table>

See “Modifying a license deployment policy” on page 251.

Deployment Policy Summary (modify) options

Use this panel to view the details of the information that you have provided in the Change thresholds of license deployment policy options panel. You can view the Low watermark and the High watermark values that you have modified.

See “Modifying a license deployment policy” on page 251.

Updating the default virtual machine count factor in Veritas Operations Manager

To update the default factor for counting the licenses that are deployed on one or more virtual systems, you can use the Update counting factor for virtual environment wizard panel.

Currently, the default factor for the Windows virtual host is four. Symantec count the licenses that are deployed on four virtual machines as one license. The licenses that are deployed on two UNIX virtual machines are counted as one license. For UNIX, the default factor is two.
To update the default virtual machine count factor in Veritas Operations Manager

1 Select Licenses > Deployment Summary.
2 In the License Deployment Summary view, click Product-Tier Mapping.
3 In the left-side panel, under All Tasks, click Update counting factor for virtual environment.
4 In the Update counting factor for virtual environment wizard panel, update the default count for UNIX or the Windows system, and click OK.
   See “Update counting factor for virtual environment options” on page 255.
5 In the Result panel that confirms the action, click OK.

Update counting factor for virtual environment options

Use this panel to update the default factor that Symantec uses for counting the licenses that are deployed on one or more virtual machines.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factor for UNIX virtual machine</td>
<td>Choose the appropriate number from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>By default, the current factor for the UNIX virtual machine is selected.</td>
</tr>
<tr>
<td>Factor for Windows virtual machine</td>
<td>Choose the appropriate number from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>By default, the current factor for the Windows virtual machine is selected.</td>
</tr>
</tbody>
</table>

See “Updating the default virtual machine count factor in Veritas Operations Manager” on page 254.

Removing a license deployment policy

You can remove a license deployment policy that you no longer require.

To remove a license deployment policy

1 In the Veritas Operations Manager console, select Licenses > Deployment Policy.
2 In the License deployment policies view, check the check box for the deployment policy that you want to remove and click Remove Policy.
3  In the Veritas Operations Manager - Remove deployment policy panel, click Yes.

4  In the Results panel, click OK.

See “Creating a license deployment policy” on page 248.

See “Modifying a license deployment policy” on page 251.
Viewing deployment information in Veritas Operations Manager

This chapter includes the following topics:

- About License Deployment Summary view
- About the product inventory summary
- About the product-tier mapping summary
- About the Tier-Host Mapping summary
- About License Deployment detailed view
- About the exceptions summary
- Viewing the License Deployment Summary view
- Viewing the summary of product inventory
- Viewing the Product-Tier Mapping summary
- Viewing the Tier-Host Mapping summary
- Viewing a product overview
- Viewing product details by host name
- Viewing the evidence details of a feature in Veritas Operations Manager
- Viewing the overview of a host
- Viewing the overview of the licenses information for a host
About License Deployment Summary view

The License Deployment Summary view is divided into the following views:

- **Summary**
- **Product Inventory**
- **Product-Tier mapping**
- **Tier-Host Mapping**
- **Exceptions**

The Summary view includes the following:

<table>
<thead>
<tr>
<th>Display</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Deployment summary table</td>
<td>Lets you view the summary of deployment licenses in the datacenter.</td>
</tr>
<tr>
<td>Summary by Product bar chart</td>
<td>Lets you view the number of licenses that are deployed in the datacenter for each Storage Foundation and high availability product.</td>
</tr>
<tr>
<td>Summary by platform bar chart</td>
<td>Lets you view the number of product licenses that are deployed in the datacenter for various platforms of Storage Foundation.</td>
</tr>
<tr>
<td>Summary by edition bar chart</td>
<td>Lets you view the number of product licenses that are deployed in the datacenter for various editions of Storage Foundation.</td>
</tr>
<tr>
<td>Summary by release bar chart</td>
<td>Lets you view the number of product licenses that are deployed in the datacenter for various releases of Storage Foundation.</td>
</tr>
</tbody>
</table>
Host deployment summary table

Lets you view the summary of deployment licenses on the hosts in the datacenter.

The Product Inventory view lets you view host-level and product-level deployment issues. It displays the types of products, the platforms they are running on, their editions, their release versions, and the price tiers to which they belong. You can also click the link under the Inventory tab to sort the view by All products, Edition, Release, and Platform.

The Product-Tier tab lets you view the following:

- Deployments by Server Price Tier
  Displays the Server Price Tier information that is categorized using the alphabets A to N.

- Deployments by Processor Type Price Tier
  Displays the information on processor type price tier.

- Deployments by NProcessors Price Tier
  The information in the Deployments by NProcessors Price Tier represents the number of processors available.

- Deployments by Installed OS Price Tier
  The information in the Deployments by Installed OS Price Tier represents the particular version of the operating system.

The Tier-Host Mapping tab lets you find the match type for each host. It displays the matrix for each Price Tier, such as the number of exact matches, number of best matches, and the number of times the users defined the match.

The Exceptions tab displays the list of hosts that are not considered in counting the license deployments.

The exception can be because of any of the following:

- Licenses for Storage Foundation and Storage Foundation-HA are not found.
- License deployment discovery that is failed to run.
- License deployment discovery is in progress.

See “About License Deployment Report” on page 234.

About the product inventory summary

The Product Inventory summary lets you view product-level and host-level deployment information.

The Product Inventory summary has the following headings. To display the information under a heading, click the arrow to its right.
What are Price Tiers?
Describes price tier levels and tier types

What are Valid, Invalid Licenses?
Displays the number of hosts, number of licenses, valid licenses, invalid licenses, and the licenses which need verification

Inventory
Filters the Product Inventory summary table by edition, release, or platform

Below the headings is the Product Inventory table. You can click any link under the Product heading to see details about the product version, host, and licenses.

You can also review tabs such as Product-Tier Mapping, Tier-Host Mapping, and Exceptions.

See “About License Deployment Summary view” on page 258.
See “Viewing the License Deployment Summary view” on page 263.
See “Viewing the summary of product inventory” on page 267.
See “About assigning price tiers to hosts” on page 240.

About the product-tier mapping summary

You can use the product-tier mapping summary to review the products that are classified by price tiers. You can click any product under Product Name to review the product overview details. These details include the number of licenses, the valid licenses, the invalid licenses, and licenses that need verification.

You can also view the price tier legend under What are Price Tiers? for more information about the types of price tiers and tier types.

The Deployment Summary can be viewed in the following ways:

- Deployments by server price tier
- Deployments by processor type price tier
- Deployments by number of processors price tier
- Deployments by installed operating system price tier

Tier types are classified into the following:

- Server
  The price is based on the make and model of the server. For example, the per-tiered-server meter is used to price and license the Veritas Storage and Server Management, High Availability products on UNIX (Solaris, HP-UX, and AIX). The price is independent of the number of domains available on the
server. You can sell UxRT products with the per-tiered-server-pricing meter or with the per-tiered-processor-pricing meter.

- **Processor type**
  The price is based on the processor type. For example, Veritas Storage and Server Management, High Availability products on UNIX can be licensed and priced per tiered processor. The per-tiered-processor price depends on the processor price tier to which a processor.

- **NProcessors**
  The price is based on the number of processors. For example, Storage and Server Automation, High Availability products on Linux are licensed on a per-processor basis. This price does not depend on the number of cores available on the processor. A multicore chip with “n” number of cores counts as one processor. For example, a dual-core AMD Opteron processor that runs Storage Foundation for Linux requires one processor license.

- **Installed operating system**
  The price is based on the installed operating system. For example, Storage and Server Automation, High Availability products on Microsoft Windows are priced per server. The price depends on the edition of Windows that is installed; for example, NT or 2000. The price does not depend on the processor capacity of the server.

See “About License Deployment Summary view” on page 258.

See “Viewing the License Deployment Summary view” on page 263.

See “Viewing the Product-Tier Mapping summary” on page 269.

See “About Symantec Licensing and Pricing” on page 237.

### About the Tier-Host Mapping summary

The Tier-Host Mapping summary lets you identify the exact match, best match, no match, and user-defined match licenses on your hosts. For example, suppose you have five Storage Foundation licenses of Tier A on five of your hosts. You are charged for those five licenses. However, when you check the Tier-Host mapping summary, you discover that you have six licenses. This may mean that you have overdeployed the same license or product on another host.

The Tier-Host Mapping summary has the following headings. You can display (or hide) the information under a heading by clicking the arrow to its right.

- **What are Price Tiers?**
  Describes price tiers and tier types.

- **Tier-Host Mapping**
Displays a table listing hosts which have the exact match, best match, no match, and user-defined match. In the far right column, you can click the icon under Comments to view information about host deployment.

See “About License Deployment Summary view” on page 258.
See “Viewing the License Deployment Summary view” on page 263.
See “Viewing the Tier-Host Mapping summary” on page 271.

About License Deployment detailed view

You can view license deployment detailed reports for platform, release, edition, hosts, and licenses. In addition, you can view the following license deployment reports:

Use the Exceptions tab to review host-level deployment issues. The Exceptions tab helps you to determine if any hosts have an invalid license. You can view host-level exceptions that are not shown on the Product Inventory tab, such as multiple or higher version licenses.

In the Overview view, you can view a product’s name, edition (for example, Enterprise, Standard), platform (for example, SunOS, Linux, AIX), and version (for example, 4.1, 5.0). You can also view the price tier, the number of hosts, the number of licenses, the invalid licenses, the expired licenses, and licenses which need verification.

You can also view product details by host name and license key.

- Product details by host name
  View details including the platform, operating system type, model, processor type, number of processors, match type, number of licenses, number of invalid licenses, and product evidence. The details also provide tier information such as the server tier, the processor tier, the number of processor tier, and the operating system tier.

- Product details by license key
  View details including the product name, platform name, license key serial number, edition, version, type, number of hosts, and the features that are enabled in the license key.

Under Product Evidence, you can click the icon to view details of the features that are enabled in the license key. Product Evidence details also provide evidence of the features on the host. You can view the product name and product version number of the products that are installed on the host. You can also view name of the enabled features, the status of enabled features, the product name to which the feature belongs, the package, the product marker file, and the number of objects.
Note: The version of the product that you have installed may be different from
the version of the product for which you have the license.

See “About License Deployment Report” on page 234.
See “About License Deployment Summary view” on page 258.
See “Viewing the License Deployment Summary view” on page 263.

About the exceptions summary

The Exceptions tab lets you review the host-level deployment issues.
The hosts that are not listed in License Deployment Report table displays the
following information:
- The hosts on which no licenses are deployed.
- The hosts on which the license discovery did not occur.

See “Viewing the summary of exceptions” on page 284.
See “About the product inventory summary” on page 259.
See “About Symantec Licensing and Pricing” on page 237.

Viewing the License Deployment Summary view

The License Deployment Summary view displays the following:
- The License deployment summary table that contains the information about
  the licenses that are deployed on various storage products in your datacenter.
- The Summary by product section that contains the information on the licenses
  for each of the Storage Foundation and the Storage Foundation-HA product
  that are deployed in your datacenter.
- The Summary by Platform section that contains the information on the licenses
  for the Storage Foundation and the Storage Foundation-HA products
  that are deployed on the hosts that run on various platforms.
- The Summary by Edition section that contains the information on the licenses
  for various editions of the Storage Foundation products.
- The Summary by Release section that contains the information on the licenses
  for various releases of the Storage Foundation products.
- The Host deployment summary table that contains the information about
  the hosts on which the Storage Foundation licenses are deployed.
**Note:** From the License Deployment Summary view, you can scope the license deployment views for the business entities using Change scope available on the top-left corner of the page.

The License deployment summary table displays the following information:

<table>
<thead>
<tr>
<th><strong>Total deployments</strong></th>
<th>Total number of license deployments in your environment. Click the number to view the details of the mapping between the deployed licenses and the hosts.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accountable deployments</strong></td>
<td>The total number of licenses for which you are accountable. If you have multiple licenses for a product with different versions deployed on a host, the version of the corresponding package is considered to mark the license as accountable. For example, if you have deployed Storage Foundation 5.0 and Storage Foundation 5.1 on one of your hosts, Storage Foundation 5.1 license is marked as accountable if VRTSvxvm 5.1 is installed on the host. Click the number to view the details of the mapping between the deployed licenses and the hosts.</td>
</tr>
<tr>
<td><strong>Keyless deployments</strong></td>
<td>The number of keyless licenses that are deployed in the datacenter. Click the number to view the details of the keyless deployments.</td>
</tr>
<tr>
<td><strong>Unique licenses</strong></td>
<td>The number of unique licenses that are deployed in the datacenter. Click the number to view the details of the unique licenses.</td>
</tr>
<tr>
<td><strong>Expired licenses</strong></td>
<td>The number of expired licenses in the datacenter. Click the number to view the details of the expired licenses.</td>
</tr>
<tr>
<td><strong>Verification needed</strong></td>
<td>The number of licenses that need to be verified. If a permanent license is installed on multiple hosts, it needs to be verified. However, you can install a site license on multiple hosts.</td>
</tr>
</tbody>
</table>
**Violated deployment policies**

Deployment policies that are violated. Click the number to view the details of the violated deployment policies.

The **License Deployment Summary** view displays the following bar charts:

**Summary by product**

This bar chart displays the number of licenses that are deployed in the datacenter for each Storage Foundation and high availability product. Click the bar chart to view the details under the Product Inventory tab. Also, this bar chart displays the total license deployment and the expired license deployments.

The **Others** category in this bar chart represents the number of licenses for CoreTech and CC Stor.

**Note:** In the bar charts, the green color represents valid licenses and the red color represents expired licenses. The number of licenses that are displayed on the chart is equal to the total number of licenses that are deployed in the datacenter.

**Summary by platform**

This bar chart displays the number of product licenses that are deployed in the datacenter for the following platforms:

- Linux
- Sun OS
- AIX
- HP-UX
- Windows.

Click the bar chart to view the details under the Product Inventory tab.

**Note:** The number of licenses that are displayed on the chart is equal to the total number of licenses that are deployed in the datacenter.
Summary by edition

This bar chart displays the number of product licenses that are deployed in the datacenter for the following editions:
- Basic
- Standard
- Enterprise
- Others.

Click the bar chart to view the details under the Product Inventory tab.

The Others category in this bar chart represents the number of licenses that do not belong to the Basic edition, Standard edition, or the Enterprise edition categories.

Note: The number of licenses that are displayed on the chart is equal to the total number of licenses that are deployed in the datacenter.

Summary by release

This bar chart displays the number of product licenses that are deployed in the datacenter for the following releases of Storage Foundation:
- 4.0
- 4.1
- 4.2
- 4.3
- 5.0
- 5.1
- Others.

Click the bar chart to view the details under the Product Inventory tab.

The Others category in this bar chart represents the number of licenses that do not belong to the releases 4.0, 4.1, 4.2, 4.3, 5.0, and 5.1.

Note: The number of licenses that are displayed on the chart is equal to the total number of licenses that are deployed in the datacenter.

The Host Deployment Summary table displays the following information:
The number of hosts in the datacenter on which the product licenses are deployed. Click the number in this column to view the details of the hosts.

Virtual hosts
The number of virtual hosts in the datacenter on which the product licenses are deployed. Click the number in this column to view the details of the virtual hosts.

Hosts with keyless licenses
The number of hosts on which the keyless licenses are deployed. Click the number in this column to view the details of the hosts that contain keyless licenses.

Hosts with expired licenses
The number of hosts that contain expired Demo licenses. Click the number in this column to view the details of the hosts that contain the invalid licenses.

Exceptions
The exception counts represent the number of hosts that belong to the exception category. The licenses for a Storage Foundation and Storage Foundation-HA can move to this state if:

- The licenses are not found on the hosts
- The license deployment discovery fails to run on the hosts
- The license deployment discovery on the hosts is still in progress

Click the number to go to the exceptions details page.

To view the License Deployment Summary

- In the Veritas Operations Manager console, select Licenses > Deployment Summary.

See “About License Deployment Summary view” on page 258.

Viewing the summary of product inventory

The product inventory details lets you view valid, invalid, and expired licenses. You can review tabs such as Product-Tier Mapping, Tier-Host Mapping, and Exceptions. However, you cannot view host-level deployment issues such as multiple licenses or higher version licenses from the product inventory view.
Under Product Inventory tab, you can view the following tables:

**What are Price Tiers**
Explains the price tiers that are used to license and price the Storage Foundation and Storage Foundation HA products.

**Description of terms used...**
Explains the names of the important columns used in the Inventory table.

**Inventory**
Explains the product inventory details.

The Inventory table displays the following:
- Product name (for example, Storage Foundation, Cluster Server)
- Platform (for example, SunOS, Linux, AIX)
- Edition (for example, Enterprise, Standard)
- Release (for example, 4.1, 5.0)
- Type of tier classification (Server tier, Processor tier, NProcessor tier, or OS tier)
- Number of hosts. You can click the number in this column to view the details in the **Hosts having license deployed** table.
- Number of licenses. You can click the number in this column to view the details in the **Licenses deployed** table.
- Number of licenses that are valid. You can click the number in this column to view the details in the **Licenses deployed** table.
- Number of licenses that are not valid. You can click the number in this column to view the details in the **Licenses deployed** table.
- Number of licenses that are deployed on multiple hosts.

The left-side panel provides you the options to filter the Inventory table.

You can enter one of the following in the **Search** text box at the top of the left-side panel to filter the **Inventory** table:
- Product name
- Processor tier
- OS tier

Also, the left-side panel displays the following categories that lets you filter the Inventory table:
- **Platform**
Edition

Release

Under each category, you can use the options to filter the table.

To view the Product Inventory summary

1. In the Veritas Operations Manager console, select Licenses > Deployment Summary.
2. In the License Deployment Summary view, click the Product Inventory tab.

See “About License Deployment Summary view” on page 258.

See “Viewing the License Deployment Summary view” on page 263.

See “About the product inventory summary” on page 259.

Viewing the Product-Tier Mapping summary

The Product-Tier Mapping summary lets you view the products that are classified according to a specific Symantec price tier. This view displays only the accountable licenses for the products that are deployed in your datacenter.

Symantec uses the following price tiers:

- Server price tier
- Processor price tier
- Operating system (OS) price tier
- NProcessor price tier

Also, Veritas Operations Manager displays the products that are not based on Symantec price tiers in the Unknown column.

You can click any product link under Product Name to see product details. You can view whether the product's license is valid, invalid, expired, or required verification.

The following table explains the Symantec price tiers that apply to the hosts using various operating systems:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Server tier</th>
<th>Processor tier</th>
<th>OS tier</th>
<th>NProcessor tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 16-1  Price tier - Operating system mapping (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Server tier</th>
<th>Processor tier</th>
<th>OS tier</th>
<th>NProcessor tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris, AIX, and HP-UX</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Virtual Linux</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Virtual Solaris</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Virtual AIX</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Virtual HP-UX</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Windows</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Virtual Windows</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
</tbody>
</table>

In Deployments by Server Price Tier, you can view the following:
- Product name
- Platform
- Product edition
- Version
- Type
- Server price tier details

In Deployments by Processor Type Price Tier, you can view the following:
- Product name
- Platform
- Product edition
- Product release
- Processor type price tier details.

In Deployments by NProcessors Price Tier, you can view the following:
- Product name
- Platform
- Product edition
- Version
- Type
NProcessors price tier details.

In Deployments by OS Price Tier, you can view the following:
- Product name
- Platform
- Product edition
- Version
- Operating system price tier details.

To view the Product-Tier Mapping summary
1. In the Veritas Operations Manager console, select **Licenses > Deployment Summary**.
2. In the **License Deployment Summary** view, click the **Product-Tier Mapping** tab.

See “About License Deployment Summary view” on page 258.
See “Viewing the License Deployment Summary view” on page 263.
See “About the product-tier mapping summary” on page 260.

Viewing the Tier-Host Mapping summary

Tier-Host mapping lets you find the match type for each host. Tier-Host mapping displays the matrix for each price tier, the number of exact matches, the number of best matches, and the number of times the users defined the match.

To view the Tier-Host Mapping summary
1. In the Veritas Operations Manager console, select **Licenses > Deployment Summary**.
2. In the **License Deployment Summary** view, click the **Tier-Host Mapping** tab.

See “About License Deployment Summary view” on page 258.
See “Viewing the License Deployment Summary view” on page 263.
See “About the Tier-Host Mapping summary” on page 261.

Viewing a product overview

The Product Overview view displays the following information:
- Product name
Viewing deployment information in Veritas Operations Manager

Viewing product details by host name

- Edition (for example, Enterprise or Standard)
- Platform (for example, SunOS, Linux, or AIX)
- Version (for example, 4.1, or 5.0)
- Price tier
- Number of hosts
- Number of licenses
- Expired licenses
- Licenses that need verification

You can also review the following tabs:

- Hosts
- Licenses
- Licenses-Hosts Mapping

To view a product overview:

1. In the Veritas Operations Manager console, select Licenses > Deployment Summary.
2. In the License Deployment Summary view, click Product Inventory.
3. In the Inventory view, under Product, click the product name.

See “About License Deployment detailed view” on page 262.
See “Viewing product details by host name” on page 272.
See “Viewing product details by license key” on page 279.

Viewing product details by host name

In the Hosts having license deployed table, you can view the following details of the hosts in the datacenter on which the license are deployed:

- Name of the host
- Platform
- Operating system
- Whether the host is a virtual machine
- Model
- Processor type
- Server Tier
- Processor Tier
- NProcessor Tier
- Operating system Tier
- NProcessors
- Match type
- Number of unique licenses
- Number of expired licenses
- Multiple Licenses
- Number of Keyless Licenses
- Product Evidence

You can click the icon under **Product Evidence** to view the details of the features that the license key enables and the hosts on which these features are available. You can view the name and the version number of the products that are installed on the host. You can also view name of the enabled features, status of enabled features, product name to which the feature belongs, package, product marker file, and number of objects.

You can use the **Assign Price Tier** option to assign a new price tier to the hosts.

The left-side panel provides you the options to filter the list of hosts that are displayed on the **Hosts having license deployed** table.

You can enter one of the following in the **Search** text box at the top of the left-side panel to filter the table:

- Host name
- Processor tier
- OS tier

Also, the left-side panel displays the following categories that lets you filter the **Hosts having license deployed** table:

- **Platform**
- **Virtual machine**
- **Tier match**
- **Licenses**

Under each category, you can use the options to filter the table.
To view product details by host name

1. In the Veritas Operations Manager console, select **Licenses > Deployment Summary**.
2. In the **License Deployment Summary** view, click **Product Inventory**.
3. In the **Inventory** view, under **Product**, click the product name.
4. Click the **Hosts** tab to view the **Hosts having license deployed** table.
   You can use the left-side panel to filter the data in the **Hosts having license deployed** table.

See “Viewing the evidence details of a feature in Veritas Operations Manager” on page 274.
See “About License Deployment detailed view” on page 262.
See “Viewing the overview of a host” on page 275.
See “Viewing the summary of product inventory” on page 267.

### Viewing the evidence details of a feature in Veritas Operations Manager

In the **Evidence Details** view, you can view the details of the features that a license key enables. Also, the **Evidence Details** view displays the evidence of the features that are present on a host.

The **Evidence Details** view displays the details in a table. At the top of the table, you can view the following information:

- Name of the host on which the licenses are deployed.
- Product that is installed on the host.
- Version of the product that is installed on the host.

The table that lists the evidence details displays the following information:

- Name of the product for which the evidence details are listed.
- Features of the product that the license key enables.
- Feature tracking information on the usage of the feature.
- Number of the storage objects that are associated with the feature.
- Package to which the feature belongs.

In the **Feature tracking** column of the **Evidence Details** view, you can view the following information for each feature:
Number of times the feature was used in the previous day.

Number of times the feature was used in the previous month.

Date and time when the feature was used last.

**To view the evidence details of a feature in Veritas Operations Manager**

1. In the Veritas Operations Manager console, select **Licenses > Deployment Summary**.
2. In the **License Deployment Summary** view, click the **Product Inventory** tab.
3. In the **Product Inventory** view, in the **Inventory** table, click the name of the product.
4. In the details view of the product, click the **Hosts** tab to view the list of hosts on which the licenses are deployed.
5. Select the option on the left-hand side to select a specific host for which you want to view the feature evidence details.
6. Under **Product Evidence** column, click the icon to view the feature evidence details.
7. In the **Evidence Details** panel, view the details of the feature that the license key enables.

See “**Viewing product details by host name**” on page 272.

**Viewing the overview of a host**

A host contains the central processing unit on which applications run and database transactions occur. In a typical storage network, hosts provide access to storage in one of the following ways:

1. **Physical storage devices**, which are attached directly to the host.
2. **Logical storage structures**, which are mapped to physical storage resources on the network.

**To view the overview of a host**

1. In the Veritas Operations Manager console, select **Manage > Hosts**.
2. In the **Host** view, select the check box for the host, which you want to overview.
3. In the **Host Details** view, review the following information related to the selected host.

**Overview**: You can select a single host and view detailed information about it. SF Manager displays the host’s name, management state, IP address, and
group membership, if any. It also displays whether it is managed in Veritas Volume Manager, replicated by Veritas Volume Replicator, or part of a Veritas Cluster Server.

See “Viewing the overview of a host” on page 275.

- **Disks**: View information about the disk on the selected host. View the disk group to which the disk belongs along with the disk’s type, status, sharing capabilities, vendor, and volume information.

- **Disk Groups**: View information about any disk groups on the selected host. View the disk group’s status, type, size, free space, version, number of disks, and number of volumes.

- **Volumes**: View information about volumes on the selected host. View the volume layout, Mount Point location of the file system, file system type, free space, usage, and the name of the volume for which a snapshot contains a point-in-time copy of its data.

- **File Systems**: View information about file systems on the selected host. View the Mount Point or location of the file system along with file system type, capacity, available storage, and usage.

- **Service Groups**: Administrators can view information about the service group, such as its state, type, family, hosts, version, cluster name, failover order, and auto start status.

- **Initiators**: View the initiators associated with the host.

- **LUNs**: View information about the logical unit numbers (LUNs) on the selected host. LUNs represent a unique and discrete addressable unit or logical volume that may reside inside one or more simple or array storage devices.

- **VCS attributes**: View all the VCS attributes that are associated with the host.

- **Host attributes**: View the host attributes. For instance, enclosure attributes, DMP attributes, and VxVM attributes.

- **Licenses/Packages**: View information about software licenses on the selected host. View the product’s name, the type of license (for example, demo or permanent), the license key information, serial number, and any licensed product features. View information about packages that are installed on the selected host. Packages can include applications, utilities, system options, or manual pages for applications. View the type of package (for example, application, option, utility or feature), and version number.

- **Available patches**: View information about the available patches on the selected host. View the product’s name, the patch type (for example, rolling patch or patch), the size of the patch file, the products on which the patch is
applicable, the release date of the patch, the release name of the patch, and the status of the patch (i.e. active or obsolete).

- **Performance**: View the performance of the host using interactive graph. See “Viewing the performance graphs for a host” on page 162.

See “About License Deployment detailed view” on page 262.

See “Viewing product details by host name” on page 272.

See “Viewing the summary of product inventory” on page 267.

### Viewing the overview of the licenses information for a host

This view provides you an overview of the licenses that are installed on a host in your datacenter.

This view displays the following information:

<table>
<thead>
<tr>
<th>Overview</th>
<th>Name of the host that you have selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Platform on which the host runs</td>
</tr>
<tr>
<td>Platform</td>
<td>Model of the platform</td>
</tr>
<tr>
<td>Model</td>
<td>Number of processors for the host</td>
</tr>
<tr>
<td>NProcessor</td>
<td>Tier that is identified based on the processor type information.</td>
</tr>
<tr>
<td>Processor Tier</td>
<td>Tier that is identified for the installed operating system. This field is applicable only for the Windows hosts.</td>
</tr>
<tr>
<td>OS Tier</td>
<td>Actual product installed on the host.</td>
</tr>
<tr>
<td>Actual Installed Product</td>
<td>Version of the product that is installed on the host</td>
</tr>
<tr>
<td>Installed Product Version</td>
<td>Operating system on which the host runs</td>
</tr>
<tr>
<td>OS</td>
<td>Specifies whether the host is a virtual machine</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Type of the processor for the host</td>
</tr>
<tr>
<td>Processor Type</td>
<td></td>
</tr>
</tbody>
</table>

Viewing deployment information in Veritas Operations Manager

Viewing the overview of the licenses information for a host
**Server Tier**

Tier that is identified based on the server information. This field is applicable only for the hosts that run on Solaris, AIX, and HP-UX.

**NProcessor Tier**

Tier that is identified based on the number of processors of the host. This field is applicable only for the Linux hosts.

**Match Type**

Indicates the way the tier was identified for the host. The available types are Exact match, Best match, and No match.

**Highest License**

Highest license that is installed on the host

**Product Evidence**

Evidence of featured on the host. Click on the corresponding icon to view the details of the product evidence.

### Licenses Deployed

- **License Key**
  License key for the product
- **Product**
  Name of the product
- **Keyless**
  Specifies whether the license is keyless
- **Serial No.**
  Serial number of the license
- **Accountable**
  Specifies whether the license is accountable
- **Platform**
  Platform for the product
- **Product Edition**
  Edition of the product
- **Version**
  Version of the license
- **Type**
  Type of the license
- **Site License**
  Specifies whether the license is a site license. Site licenses can be installed on multiple hosts.
- **VVR Option**
  Specifies whether Veritas Volume Manager option is enabled
- **OEM ID**
  Identification number of the Original Equipment Manufacturer
- **Expiration Date**
  Date on which the license expires
### Days Remaining
Number of days within which the license is expired

### Child Licenses
Child licenses for the product license. Child Licenses are the licenses that are installed through Edition products.

Click on the corresponding icon to view the details.

### Feature Enabled
Features that are enabled by this license.

Click on the icon to view the details of the features enabled by this license.

Click on the corresponding icon to view the details.

---

**To view the overview of the licenses information for a host**

1. In the Veritas Operations Manager console, click **Licenses > Deployment Summary**.

2. In the **Host deployment summary** table, click the number in the **Total Hosts** column.

3. In the **Hosts** tab, click on a host to view its overview.

See “Viewing the License Deployment Summary view” on page 263.

---

### Viewing product details by license key

**The Product Inventory** tab lets you view product details by license key.

The details include the following:

- License key
- Product
- Keyless
- Serial No.
- Platform
- Edition
- Version
- Type
- Site Licenses
- VVR Option
- OEM ID
- Number of hosts
- Expired licenses on hosts
- Child Licenses
- Features enabled

You can click the icon under **Features Enabled** to view the name of each feature, the status of the enabled feature, and the product to which the enabled features belong.

**Note:** Windows managed hosts do not contain any child licenses.

The left-side panel provides you the options to filter the **Licenses deployed** table. You can enter the product name or the license key in the **Search** text box at the top of the left-side panel to filter the **Licenses deployed** table.

Also, the left-side panel displays the following categories that lets you filter the **Licenses deployed** table:
- Platform
- Edition
- Release
- License attributes
- Licenses that need verification

Under each category, you can use the options to filter the table.

**To view product details by license key**

1. In the Veritas Operations Manager console, select **Licenses > Deployment Summary**.
2. In the **License Deployment Summary** view, click **Product Inventory**.
3. In the **Inventory** table, under **Product**, click the product name.
4. Click the **Licenses** tab and view the details that are displayed on the **Licenses deployed** table.

See “**About License Deployment detailed view**” on page 262.

See “**Viewing License Key details**” on page 281.

See “**Viewing the summary of product inventory**” on page 267.
Viewing License Key details

You can view license key details including the license key number; the product name, edition, version and type; the license and product expiration dates; the number of days before the product license expires; the status of license expiration; the status of deployment; the number of hosts; and the features enabled.

To view license key details

1. In the Veritas Operations Manager console, select Licenses > Deployment Summary.
2. In the License Deployment Summary view, click Product Inventory.
3. In the Inventory view, under Product, click the product name.
4. Click the Licenses tab.
5. Under License Key, click the license key number link.
6. View detailed host information:

   - **Features Enabled**: Click the icon to display enabled features, their status, and the product to which they belong.
   - **Hosts having license deployed**: Click the links to sort hosts by platform, license matches, or types of license. You can use the Assign Price Tier button to assign a new price tier to hosts.
   - **License detail table**: Displays license key details including the host name, platform, server tier, processor tier, number of processors tier, operating system tier, operating system, model, processor type, number of processors, match type, number of licenses, number of invalid licenses, whether the product corresponding to license key is installed, comments, and product evidence.
   - **Product Evidence**: Displays the features that are enabled in the license key and evidence of features on the host. You can view the names and version numbers of the products installed on the host. You can also view the name and status of enabled features, the product to which the feature belongs, the package, marker file, and the number of objects.
Viewing the details of the mapping between the licenses and hosts

The Licenses-Hosts Mapping view displays detailed product information including the following:

- License key
- Product name
- Version (for example, 4.1, 5.0)
- Edition (for example, Enterprise, Standard)
- License expiration date (for example, 2008-08-05)
- Days until the license expires

To view product details by license-host mapping

1. In the Veritas Operations Manager console, select Licenses > Deployment Summary.
2. In the License Deployment Summary view, click the Product Inventory tab.
3. In the Inventory view, under Product, click the product name.
4. Click the Licenses-Hosts Mapping tab.

See “About License Deployment detailed view” on page 262.
See “Viewing a product overview” on page 271.
- Accountable licenses
- Version (for example, 4.1, 5.0)
- Edition (for example, Enterprise, Standard
- License type
- License expiration date (for example, 2008-08-05)
- Days until the license expires
- Host on which the license is deployed
- Operating system of the host
- Whether the host is a virtual machine
- Server tier details
- Processor tier details
- NProcessor tier details
- OS tier details
- Match type
- Child licenses
- Features that the license key enables.

The left-side panel provides you the options to filter the **Licenses-Hosts Mapping** table.

You can enter one of the following in the **Search** text box at the top of the left-side panel to filter the **Licenses-Hosts Mapping** table:

- Host name
- Product name
- Processor tier
- OS tier

Also, the left-side panel displays the following categories that lets you filter the **Licenses-Hosts Mapping** table:

- Platform
- Virtual Machine
- Edition
- Release
- Expired licenses
- Keyless licenses
- Accountable licenses

Under each category, you can use the options to filter the table.

**To view product details by license-host mapping**

1. In the Veritas Operations Manager console, select **Licenses > Deployment Summary**.
2. In the **License Deployment Summary** view, click the **Product Inventory** tab.
3. In the **Inventory** view, under **Product**, click the product name.
4. Click the **Licenses-Hosts Mapping** tab and view the details that are displayed on the **Deployed License-Host Mapping** table.

See “About License Deployment detailed view” on page 262.

See “Viewing a product overview” on page 271.

**Viewing the summary of exceptions**

The **Exceptions** tab lets you review the host-level license deployment issues that cannot be reviewed through the **Product Inventory** view. You can view the list of hosts on which licenses were not found or the license discovery was failed.

**To view the Exceptions summary**

1. In the Veritas Operations Manager console, select **Licenses > Deployment Summary**.
2. In the **License Deployment Summary** view, click the **Exceptions** tab.

See “About License Deployment detailed view” on page 262.

See “About the exceptions summary” on page 263.

**Viewing the VOM Management Entitlement Report**

This view provides you detailed information on the licenses that your hosts require in case they report to Veritas Operations Manager Enterprise Server. If the Management Server in your environment reports to the Veritas Operations Manager Enterprise Server, only the hosts that run Storage Foundation Standard or Storage Foundation Basic require valid licenses. If the Management Server does not report to the Veritas Operations Manager Enterprise Server, only the hosts that do not run Storage Foundation, Veritas Cluster Server, or Dynamic Multipathing require valid licenses.
The **Overview** section in this view displays the following information:

- The total number of hosts that report to Management Server.
- The number of hosts that run Storage Foundation, Veritas Cluster Server, or Dynamic Multipathing, out of the total number of hosts.
- The number of hosts that run Storage Foundation Enterprise, out of the number of hosts that runs Storage Foundation.
- The number of hosts that require the Veritas Operations Manager Advanced license, out of the total number of hosts.
  - If the Management Server reports to Veritas Operations Manager Enterprise Server, this is equal to the number of hosts that run Storage Foundation Standard or Storage Foundation Basic.
  - If the Management Server does not report to the Veritas Operations Manager Enterprise Server, this is equal to the number of hosts that do not run Storage Foundation, Veritas Cluster Server, or Dynamic Multipathing.
- The number of hosts that do not run Storage Foundation, Veritas Cluster Server, or Dynamic Multipathing, out of the total number of hosts.
- The number of hosts that have a valid license for Storage Foundation Standard or Storage Foundation Basic, out of the number of hosts that runs Storage Foundation.

Using the **Search** field on the left side of the view, you can search for a host using its name or the platform on which it runs. To search for a host, enter a part of the name or the platform in the **Search** field.

Using the filter option on the left side of the view, you can filter the selection of hosts in the **VOM Management Entitlement Report** table based on:

- The agentless hosts
- The hosts that do not run any of the Storage Foundation products
- The Enterprise, Standard, and the Basic editions of Storage Foundation

The **VOM Management Entitlement Report** table in this view displays the following details:

<table>
<thead>
<tr>
<th><strong>Host Name</strong></th>
<th>Name of the host</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform</strong></td>
<td>Operating system on which the host runs</td>
</tr>
<tr>
<td><strong>Agentless</strong></td>
<td>Indicates whether the Veritas Operations Manager agent is installed on the host</td>
</tr>
</tbody>
</table>
Indicates whether Storage Foundation, Veritas Cluster Server, or Dynamic Multipathing is installed on the host

Edition

The edition of the Veritas Operations Manager Enterprise Server.

To view the VOM Management Entitlement Report
◆ In the Veritas Operations Manager console, select Licenses > VOM Management Entitlement Report.

Scoping a license deployment view using business entities

In Veritas Operations Manager, you can scope a license deployment view by specifying business entities. You can do this task from any views that are related to license deployment.

Note: In Veritas Operations Manager, business entities comprise application and organization entities.

Scoping the license deployment views based on a specific business entity helps you focus on the deployment details of licenses that are part of that business entity.

Note: By default, Veritas Operations Manager displays the deployment details of all the licenses in the domain.

To scope a license deployment view using business entities

1 In Veritas Operations Manager console, select Licenses > Deployment Summary.

2 At the top of any license deployment view, near to the Current scope field, click Change scope.
   For example, at the top of the License Deployment Summary view, near to the Current scope field, click Change scope.

3 In the Scoping License Views wizard panel, select the business entity based on which you want to scope the license deployment view and click Finish.

See “Scoping License Views options” on page 287.
See “About License Deployment Summary view” on page 258.
See “Viewing the License Deployment Summary view” on page 263.

Scoping License Views options

Use this wizard panel to scope a license deployment view using a business entity.

**Note:** In Veritas Operations Manager, business entities comprise application and organization entities.

<table>
<thead>
<tr>
<th>Table 16-2 Scoping License Views panel options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td><strong>Entire Domain</strong></td>
</tr>
<tr>
<td><strong>Select business entity</strong></td>
</tr>
</tbody>
</table>

See “Scoping a license deployment view using business entities” on page 286.
Viewing deployment information in Veritas Operations Manager

Scoping a license deployment view using business entities
Using Policy Check

This chapter includes the following topics:

■ About Policy Check
■ About policy templates
■ About creating policy templates
■ Creating policy templates
■ Modifying policy templates
■ Running a manual policy template scan
■ Deleting a policy template
■ About policy violations
■ Marking policy violations to exclude from the subsequent scans
■ About Installed Signatures
■ About the customized signature in Veritas Operations Manager for identifying risks
■ Adding signatures to a policy template
■ Setting signature tunables
■ Removing a signature from a policy template
■ Deleting a policy template scan
■ Viewing scan tunables associated with a policy scan
■ Removing ignored violations from the ignore list
About Policy Check

The Veritas Operations Manager Policy Check uses individual rules to validate whether the datacenter configuration conforms to a pre-defined standard. These individual rules are named as signatures. You can execute the signatures across the Veritas Operations Manager environment. The policy check feature in Veritas Operations Manager lets you manage the signatures. Veritas Operations Manager contains 50 pre-defined signatures. In addition to the pre-defined signatures, Veritas Operations Manager lets you create the customized signatures.

The Veritas Operations Manager Policy Check enables the administrator to identify the resources which do not meet that specified standard, and track these violations over time. These standards can be configured to scan multiple signatures, at specific scheduled intervals, with different options, against any number of hosts in your datacenter. The Policy Check allows you to better identify and address risks in your environment by providing notification of error and risk conditions on a proactive basis, before they evolve into something more severe.

The time that is required for collecting data to generate a Policy Check report depends on the number of hosts against which the policy checks must run on, the size of the configuration, and the number of signatures run.

See “About policy templates” on page 290.

See “About Installed Signatures” on page 299.

See “About the customized signature in Veritas Operations Manager for identifying risks” on page 300.

About policy templates

Veritas Operations Manager lets you configure a policy template by specifying the signatures that must be included in the scan. You can also specify the hosts or business entities against which the scan must be run. You can also specify how frequently to run the scan i.e. daily, weekly, and so on. In short, the policy templates enable you to customize the checks on the managed objects and set the options for the checks in that template.

You cannot run the policy checks on ESX servers and non-global zones because the VRTSsfmh package is not installed on them.

Note: Users other than the Domain Administrators are only allowed to create, edit, or delete policy templates on Business Entities on which they have administrative privileges.
See “About creating policy templates” on page 291.

Table 17-1 provides details on the available policy templates.

<table>
<thead>
<tr>
<th>Policy template Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the policy template. This is an optional value.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the policy template and what it does. This is an optional value.</td>
</tr>
<tr>
<td>Scope</td>
<td>Specifies what hosts or business entities the template is run against.</td>
</tr>
<tr>
<td>Last Scan</td>
<td>Specifies the date and time and the link to the last scan that was run using this policy template.</td>
</tr>
<tr>
<td>Violations in last scan</td>
<td>Specifies the number of policy violations in the last scan.</td>
</tr>
</tbody>
</table>

The Policy Templates view also provides a filter to view the specified policy templates as per the specified criteria. This filter searches on the Name, Description, and Scope fields.

In the search box on the Filter Policy Templates panel, you can type in a search keyword.

You can click on the name of the policy template to get more information about it. This provides details about the time when the policy template was scanned, the signatures which were violated, the hosts on which the violation occurred, and the total number of violations.

For more detailed information of the policy violations resulting from a scan that is conducted on a specific date, click on the date of the scan.

For more information on policy violations:
See “About policy violations” on page 298.

About creating policy templates

You can create a policy template in the following ways:

- Creating a policy template using wizards.
  See “Creating policy templates” on page 292.
- Adding signatures to policy templates.
  See “Adding signatures to a policy template” on page 308.
Creating policy templates

Veritas Operations Manager lets you create policy templates to check the performance, availability, utilization of the storage objects in your datacenter. The policy templates also generates information based on the conformance of the storage objects with the best practices. Using the policy templates, you can scan the storage objects for 42 types of checks.

You can create policy templates only for the domains where you have administrator privileges.

To create a policy template

1. Select **Policies > Policy Templates**.
2. Click **Create Policy Template**.
3. In the **Policy Template Details** panel, enter the required information. Click **Next**.
   
   See “**Policy Template Details options**” on page 293.
4. In the **Select Signatures** panel, click the check boxes next to the signatures that you want to include in the policy template. Click **Next**
   
   See “**Select Signatures options**” on page 293.
5. If you chose to run the policy template scan on specific hosts, select the hosts in the **Select Scope** panel. This panel is not displayed if you chose to run the scan on all the hosts. Click **Next**

   See “**Select Scope options**” on page 294.
6. In the **Specify Schedule** panel, choose when to run all the signatures that are associated with the policy template. Click **Next**

   See “**Specify Schedule options**” on page 294.
7. In the **Policy Template Summary** panel, confirm the selections that you made to create the policy template.

   See “**Policy Template Summary options**” on page 295.
8. Click **Finish** to create the policy template.
9. In the **Result** panel, verify that the policy template was successfully created. Click **OK**.

See “**About policy templates**” on page 290.

See “**Deleting a policy template**” on page 297.
Policy Template Details options

Use this wizard panel to specify the details of the policy template.

Table 17-2  Policy Template Details panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the policy template name.</td>
</tr>
<tr>
<td>Description</td>
<td>Add a brief description of the policy template.</td>
</tr>
<tr>
<td>Scan Scope</td>
<td>Select one of the following to define the scan scope:</td>
</tr>
<tr>
<td></td>
<td>• Scan specific hosts to choose the hosts to be scanned</td>
</tr>
<tr>
<td></td>
<td>• Scan hosts associated with a Business Entity to scan the hosts that are associated with a business entity</td>
</tr>
<tr>
<td></td>
<td>• Scan all hosts to scan all the hosts</td>
</tr>
<tr>
<td>Email</td>
<td>Specify the email address to which notifications must be sent in case of policy violations. This field is optional.</td>
</tr>
</tbody>
</table>

See “Creating policy templates” on page 292.

See “Modifying policy templates” on page 296.

Select Signatures options

Some signatures are packaged with a standard Veritas Operations Manager installation.

Use this wizard panel to select the signatures for the policy template.

Table 17-3  Select Signatures panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Specify keywords to filter the list of available signatures.</td>
</tr>
<tr>
<td>Selected</td>
<td>Lists all the signatures that you have selected.</td>
</tr>
</tbody>
</table>
Table 17-3  Select Signatures panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Selected</td>
<td>Removes a selected signature from the selected signatures list.</td>
</tr>
<tr>
<td>Remove All</td>
<td>Removes all the signatures from the selected signatures list.</td>
</tr>
</tbody>
</table>

See “Creating policy templates” on page 292.
See “Modifying policy templates” on page 296.

Select Scope options

Use this wizard panel to select the hosts on which to run the policy template scan. Select the check boxes to select the hosts.

Table 17-4  Select Scope panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Specify keywords to filter the list of available hosts.</td>
</tr>
</tbody>
</table>

See “Creating policy templates” on page 292.
See “Modifying policy templates” on page 296.

Specify Schedule options

Use this wizard panel to specify when the policy template scan is to be run.
Table 17-5  Specify Schedule panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td><strong>No Schedule</strong> - Select this option to indicate that you will manually run the scan as and when required.</td>
</tr>
<tr>
<td></td>
<td><strong>Daily</strong> - Select this option to run the scan once every day. You have to specify the time when the scan should be run.</td>
</tr>
<tr>
<td></td>
<td><strong>Weekly</strong> - Select this option to run the scan once every week. You can choose to run it on every weekday, or on specific weekdays. Also, you have to specify the time when the scan should be run.</td>
</tr>
<tr>
<td></td>
<td><strong>Monthly</strong> - Select this option to run the scan once every month. You can choose to run it on a particular day of the month, or on a specific weekday. Also, you have to specify the time when the scan should be run.</td>
</tr>
</tbody>
</table>

| When              | Specify the schedule for the policy template scan.                                                                                          |

See “Creating policy templates” on page 292.
See “Modifying policy templates” on page 296.

Policy Template Summary options

Use this wizard panel to confirm the selections that you made to create the policy template.

Table 17-6  Policy Template Summary panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Policy Template Scan immediately</td>
<td>Select this option to run the scan immediately after the policy template is created.</td>
</tr>
</tbody>
</table>

See “Creating policy templates” on page 292.
See “Modifying policy templates” on page 296.
Modifying policy templates

In Veritas Operations Manager, the **Edit Policy Template** option lets you make further changes to the existing policy templates.

**To modify an existing policy template**

1. In the Veritas Operations Manager console, select **Policies > Policy Templates**.
2. To modify the policy template, do one of the following:
   - Select the policy template and click **More > Edit Policy Template**.
   - Right-click the policy template and select **Edit Policy Template**.
3. In the **Policy Template Details** wizard panel, modify the required information and click **Next**.
   
   See “**Policy Template Details options**” on page 293.

4. In **Select Signatures** panel, modify the selection of the signatures if required and click **Next**.
   
   See “**Select Signatures options**” on page 293.

5. In **Select Scope** panel, modify the scope for the scan and click **Next**.
   
   See “**Select Scope options**” on page 294.

6. In the **Specify Schedule** panel, modify the frequency at which you want to run the scan and click **Next**.
   
   See “**Specify Schedule options**” on page 294.

7. In the **Policy Template Summary** panel, review the configuration details that you entered while modifying the policy template.
   
   Select the **Run Policy Template Scan immediately** check box if you want to run the policy scan immediately after you modify the policy template.
   
   See “**Policy Template Summary options**” on page 295.

8. Click **Finish**.

9. In the **Result** panel, click **OK** to confirm the changes that you have made to the policy template.
   
   See “**Creating policy templates**” on page 292.

   See “**Deleting a policy template**” on page 297.

   See “**Adding signatures to a policy template**” on page 308.

   See “**Removing a signature from a policy template**” on page 309.
Running a manual policy template scan

In Veritas Operations Manager, you can run a policy template scan manually.

To run a manual policy template scan

1. Select Policies > Policy Templates.
2. Select the check box corresponding to the policy template that you want to run manually.
3. Click Scan Now.
4. In the Run Policy Template Scan Now page, click Yes to run the scan.
5. In the Results page, verify that the policy template scan has started. Click OK.

See “About Policy Check” on page 290.
See “About policy templates” on page 290.
See “Deleting a policy template scan” on page 310.

Deleting a policy template

You can delete one or more existing policy templates if they are no more required in Veritas Operations Manager. If you delete a policy template, its associated scans and the identified policy violations are also removed permanently from the system.

Only the root user or the domain administrator can delete the policy templates.

To delete a policy template

1. In the Veritas Operations Manager console, select Policies > Policy Templates.
2. Select the policy template that you want to delete and do one of the following:
   - Click More > Delete Policy Template.
   - Right-click the policy template and from the submenu, select Delete Policy Template.
3. Click Yes to confirm.

See “About policy templates” on page 290.
See “Creating policy templates” on page 292.
See “Deleting a policy template scan” on page 310.
About policy violations

A policy violation occurs when a configuration option on a managed host does not meet the condition that a signature for the corresponding policy template sets for it.

You can scan for policy violations using the Scan Now tab on the Policy Templates view instead of waiting for the scheduled scan time (if specified). This opens a dialog box asking for confirmation to run the policy scan.

Table 17-7 displays the manner in which the results of the completed scan are classified.

<table>
<thead>
<tr>
<th>Scan operations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show New Violations</td>
<td>Indicates new policy violations in this scan that were not part of a previously run scan.</td>
</tr>
<tr>
<td>Show Resolved Violations</td>
<td>Indicates the policy violations that were found in previous scans that are no longer occurring.</td>
</tr>
<tr>
<td>Show Persisting Violations</td>
<td>Indicates the violations that occurred in previous scans and are continuing to happen in the selected scan.</td>
</tr>
<tr>
<td>Delete Scan</td>
<td>Deletes the selected scans.</td>
</tr>
<tr>
<td>Show Scan Tunables Used</td>
<td>Indicates the tunables or configurable variables associated with included signatures.</td>
</tr>
<tr>
<td>Ignored violations</td>
<td>Indicates the policy violations that the administrator has chosen to ignore.</td>
</tr>
</tbody>
</table>

See “Running a manual policy template scan” on page 297.

See “Marking policy violations to exclude from the subsequent scans” on page 298.

See “Removing ignored violations from the ignore list” on page 311.

Marking policy violations to exclude from the subsequent scans

After the policy template scan, you can view the list of all policy violations. You can mark one or more policy violations if you want to exclude them from the subsequent scans. It is referred to as ignoring the violation. Once you have marked these policy violations, they are not included in next scan cycles.
To mark a policy violation to exclude from the subsequent scans

1. In the Veritas Operations Manager console, select **Policies > Policy Templates**.

2. Click the policy template for which you want to exclude its associated policy violations in the subsequent scans.

3. Under **Scans**, you can view all the scan reports associated with the policy template that you have selected. Click the desired scan report.

4. In **Violations** table, select the violation that you want to exclude from the subsequent scans.

5. At the top of the **Violations** table, click **Ignore Violation**.

6. In the **Ignore Violations** panel, click **OK**.

7. In the **Results** panel, click **OK** to confirm.

See “About policy violations” on page 298.

See “Removing ignored violations from the ignore list” on page 311.

### About Installed Signatures

The Policy Check signatures are installed and managed centrally. Currently, there is a default set of signatures that is shipped with a basic Veritas Operations Manager installation. The **Installed Signature** view provides a global overview of the the signatures or policies that are already installed and available to you.

The **Installed Signatures** view also provides a filter to selectively view the specified signatures.

**Table 17-8** displays information about the available signatures.

<table>
<thead>
<tr>
<th>Installed Signature Information</th>
<th>Functional description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the installed signature</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description about the installed signature and what it does.</td>
</tr>
<tr>
<td>Keywords</td>
<td>Keyword or search categories that can be used in the filter to identify required signatures as per a specified criteria.</td>
</tr>
<tr>
<td>Tunable settings</td>
<td>Default configurable options or variables that can be set or adjusted for some signatures.</td>
</tr>
</tbody>
</table>
The **Set Tunables** tab displays the tunables that are associated with a signature. See “Setting signature tunables” on page 308.

The **Show Additional information** tab provides some additional information detailing what violations the signature will discover. It also suggests some possible ways to remediate that condition.

The **RemoveSignature** tab allows you to remove the specified signature from the policy template.

For more information on removing signatures:

See “Removing a signature from a policy template” on page 309.

---

**Note:** Additional signatures are distributed via a signature pack.

See “Adding signatures to a policy template” on page 308.

See “About Policy Check” on page 290.

See “About the customized signature in Veritas Operations Manager for identifying risks” on page 300.

---

**About the customized signature in Veritas Operations Manager for identifying risks**

Veritas Operations Manager lets you create customized signatures, which you can schedule to run at specified time with specified options on specified sets of hosts. As administrators, you can use the information that these customized signatures gather to address the risks in the Veritas Operations Manager environment proactively. Also, you can define notifications based on these signatures on any error conditions that may occur in your Veritas Operations Manager environment.

After you create the customized signature script, you must register the script on Management Server. Then, you must copy the customized signature script to the managed hosts where you want to run it. Also, you can use the Distribution Manager Add-on to create a customized signature script, register it on Management Server, and copy it to the managed hosts.

Apart from the 50 predefined signatures available with Veritas Operations Manager, you can plug-in the customized signatures to the policy check feature.

See “About Policy Check” on page 290.

See “About Installed Signatures” on page 299.
About creating a customized signature script

You can create the customized signature script using any programming language. Also, the customized signature script can have any type of code.

You must ensure the following when you create the customized signature script:

- Script must return 0 for success.
- Script must return a value other than 0 for errors.

In case of error, the script must print as follows:

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESULT_RC</td>
<td>Any of the following exit codes:</td>
</tr>
<tr>
<td></td>
<td>■ 0 - Check passed.</td>
</tr>
<tr>
<td></td>
<td>■ 1 - Check fails with warning.</td>
</tr>
<tr>
<td></td>
<td>■ 2 - Check fails with error.</td>
</tr>
<tr>
<td></td>
<td>■ 100 - Not supported or cannot run check.</td>
</tr>
<tr>
<td>RESULT_TXT</td>
<td>Displays the failure message</td>
</tr>
<tr>
<td>RESULT_REMEDY</td>
<td>Displays the message that helps resolve the problem.</td>
</tr>
</tbody>
</table>

The customized signature script must support the `--what` command line argument, which ensures the following output when you use the `customized_signature_script.pl --what` command:
Table 17-10  Output of the command: customized signature script.pl --what

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECK_ID</td>
<td>Displays a unique value. This value can be a number or a string.</td>
</tr>
<tr>
<td></td>
<td>Example: PC_VXVM_UNUSED_VOLUMES</td>
</tr>
<tr>
<td>CHECK_NAME</td>
<td>Displays the name of the customized signature.</td>
</tr>
<tr>
<td>CHECK_DESCRIPTION</td>
<td>Displays the description for signature.</td>
</tr>
<tr>
<td>CHECK_KEYWORDS</td>
<td>Displays the category to which the customized signature belongs.</td>
</tr>
<tr>
<td></td>
<td>Example: UTILIZATION/VXVM/PERFORMANCE/VCS</td>
</tr>
</tbody>
</table>

**Note:** The customized signature must return the code 0 on successful registration on Management Server. It must not give any other output.

See “Sample customized signature script” on page 302.

See “About the customized signature in Veritas Operations Manager for identifying risks” on page 300.

See “About registering the customized signature” on page 304.

See “About copying the customized signature script” on page 304.

See “About using the Distribution Manager Add-on to bundle a customized signature” on page 305.

See “About removing a customized signature from Veritas Operations Manager” on page 308.

**Sample customized signature script**

**Note:** The following sample script is created using PERL.

```perl
#!/opt/VRTSsfmh/bin/perl
BEGIN { @INC = ("/opt/VRTSsfmh/lib/modules"); } 
use strict;
```
if ($ARGV[0] eq "--what")
{
    print "CHECK_ID: PC_VXVM_UNUSED_VOLUMES\n";
    print "CHECK_NAME: VxVM Unused Volumes\n";
    print "CHECK_DESCRIPTION: Check to see if any VxVM volumes are unused.\n";
    print "CHECK_KEYWORDS: UTILIZATION UNIX VXVM\n";
    exit (0);
}

if($^O =~ /Win32/i)
{
    print "RESULT_RC=100\n";
    print "RESULT_TXT=Windows host detected\n";
    print "RESULT_REMEDY=This check is intended only for unix hosts\n";
    exit(100);
}

my $exitcode = 0;
my @items = `/opt/VRTSsfmh/bin/vxlist -t stats vol`; my $iocount = {};

foreach (@items) {
    if(/^vol\s+(\S+)\s+(\S+)\s+(read|write)\s+(\S+)\s+/) {
        my $name = $2."/".$1;
        $iocount->{$name} += $4;
    }
}

foreach (keys %$iocount) {
    if($iocount->{$_} == 0) {
        /(^\S+)\/(\S+)\/\s+(read|write)\s+(\S+)\s+/; 
        my $name = $2."/".$1;
        $exitcode = 2;
    }
}

exit($exitcode);

See “About creating a customized signature script” on page 301.
About registering the customized signature

After you create the customized signature, you must register it on the Veritas Operations Manager Management Server. Before you register the signature, you must ensure that the signature is in the executable format.

To register a customized signature, you can use the `pcreg` utility, which is available in the following locations:

- On UNIX Management Server - /opt/VRTSsfmh/bin
- On Windows Management Server - C:\Program Files\VERITAS\VRTSsfmh\bin

The following is the syntax that you can use for registering the customized signatures:

```
pcreg --script policy check script
```

**Note:** In this syntax, you must provide the full path to the customized signature script.

After you register the customized signature, you can view the signature in the **Installed Signatures** view. You can add this signature to an existing or a new policy template. Also, you must copy the customized signature on the managed hosts where you want to run it.

To view the customized signature that you have registered, navigate to **Policies > Signatures** in the Veritas Operations Manager console.

See “About the customized signature in Veritas Operations Manager for identifying risks” on page 300.

See “About creating a customized signature script” on page 301.

See “About copying the customized signature script” on page 304.

See “About using the Distribution Manager Add-on to bundle a customized signature” on page 305.

See “About removing a customized signature from Veritas Operations Manager” on page 308.

About copying the customized signature script

You must ensure that the customized signature exists on the managed host where you want it to run it.

You must copy the customized script to the following locations:

- On UNIX managed hosts - /opt/VRTSsfmh/lib/signatures
On Windows managed host - C:\Program Files\VERITAS\VRTSsfmh\lib\signatures

You can copy the customized signature to the managed hosts manually. Also, you can use the Distribution Manager Add-on to push the customized signatures to the required managed hosts.

See “About the customized signature in Veritas Operations Manager for identifying risks” on page 300.

See “About creating a customized signature script” on page 301.

See “About registering the customized signature” on page 304.

See “About using the Distribution Manager Add-on to bundle a customized signature” on page 305.

See “About removing a customized signature from Veritas Operations Manager” on page 308.

About using the Distribution Manager Add-on to bundle a customized signature

Using the Distribution Manager Add-on, you can bundle the signature, set up, and the unsetup scripts to a.sfa archive. The setup script can register the customized signature at a specific location on Management Server and copy the customized signature at a specific location on the managed host. Once the add-on is created for the customized signature, you can deploy it using the Deployment Management feature. The unsetup script of the add-on can unregister the customized signature on Management Server and remove the customized signature from managed hosts.

For information on using the Distribution Manager Add-on, see Veritas Operations Manager Distribution Manager Add-on 3.1 User's Guide.

See “Sample setup.pl script for the customized signature” on page 306.

See “Sample unsetup.pl script for a customized signature” on page 307.

See “About the customized signature in Veritas Operations Manager for identifying risks” on page 300.

See “About creating a customized signature script” on page 301.

See “About registering the customized signature” on page 304.

See “About copying the customized signature script” on page 304.

See “About removing a customized signature from Veritas Operations Manager” on page 308.
Sample `setup.pl` script for the customized signature

The following is the sample `setup.pl` script for the customized signature:

```
#!/opt/VRTSsfmh/bin/perl

BEGIN { @INC = ('/opt/VRTSsfmh/lib/modules'); }

use VRTS::AddOnInfo;
use File::Copy;
require File::Spec;

my $store_dir = $ENV{'Store'};
my $install_dir = VRTS::Paths::get_path("InstallDir");
my $pcregutil = File::Spec->catfile($install_dir,"bin","pcreg");
my $sigdir = File::Spec->catfile($install_dir,"lib","signatures");

# Creating array of signature files name
@signature_files = ("UnUsedVolumes.pl");

# Copy file under signatures directory
foreach $sigfile (@signature_files)
{
    print "Coping script $sigfile to $sigdir\n";
    copy($sigfile,$sigdir);

    print "Making script executable\n";
    my $pc = File::Spec->catfile($sigdir,$sigfile);
    system("chmod +x $pc");

    # Register signature only on CS
    if ( VRTS::AddOnInfo::is_CS() )
    {
        print "Registering script\n";
        my $cmd1 = VRTS::Util::make_command($pcregutil,"--script","$pc");
        system($cmd1);
    }
}
exit(0);
```

See “About using the Distribution Manager Add-on to bundle a customized signature” on page 305.
Sample `unsetup.pl` script for a customized signature

The following is the sample `unsetup.pl` script for a customized signature:

```perl
#!/opt/VRTSsfmh/bin/perl

BEGIN { @INC = ("/opt/VRTSsfmh/lib/modules"); }

use VRTS::AddOnInfo;
use File::Copy;
require File::Spec;

my $install_dir = VRTS::Paths::get_path("InstallDir");
my $sigdir = File::Spec->catfile($install_dir,"lib","signatures");
my $pcregutil = File::Spec->catfile($install_dir,"bin","pcreg");

# Creating array of signature files name and signature name
@signature_files = ("UnUsedVolumes.pl");
@signature_names = ("PC_VXVM UNUSED VOLUMES");

# Unregister script on CS
if ( VRTS::AddOnInfo::is_CS() )
{
    foreach $signame (@signature_names)
    {
        print "Unregister signature $signame\n";
        system("$pcregutil --id $signame");
    }
}

# Remove signature from signature directory
foreach $sigfilename (@signature_files)
{
    print "Remove script $sigfilename\n";
    my $sigfile = File::Spec->catfile($sigdir,$sigfilename);
    File::Path::rmtree("$sigfile");
}
exit(0);
```

See “About using the Distribution Manager Add-on to bundle a customized signature” on page 305.
About removing a customized signature from Veritas Operations Manager

To remove a customized signature from Veritas Operations Manager, you can run the following utility:

```
pcreg --id policy check id
```

See “About registering the customized signature” on page 304.

See “About using the Distribution Manager Add-on to bundle a customized signature” on page 305.

See “About the customized signature in Veritas Operations Manager for identifying risks” on page 300.

Adding signatures to a policy template

In Veritas Operations Manager, you can add signatures to a policy template in the Installed Signatures view.

To add signatures to policy templates

1. In the Veritas Operations Manager console, select Policies > Installed Signatures.

2. In the Installed Signatures view, select the check boxes for the signatures that you want to add to a policy template and do one of the following:
   - Click Add to Policy Template.
   - Right-click one of the selected signatures, and then click Add to Policy Template.

3. In the Add Signature to Policy Template panel, in the Policy Templates list, select the policy template to which you want to add the signatures and click OK.

4. In the Result panel, verify that the operation was successful and click OK.

See “About Installed Signatures” on page 299.

See “About policy templates ” on page 290.

See “Removing a signature from a policy template” on page 309.

Setting signature tunables

In Veritas Operations Manager, you can set the tunables for a signature that you selected while creating a policy check template under the Signatures tab in the
policy template details. However, some of the signatures may not have any associated tunables. You can refer to the Tunable Settings column of the Signatures table to determine whether a signature has any associated tunables.

To set signature tunables

1. In the Veritas Operations Manager console, select Policies > Policy Templates.
2. Click on the desired policy template to view the policy template details.
3. On the Signatures tab, do one of the following:
   - Select the check box for the signature for which you want to set the tunables and click Set Tunables.
   - Right-click the signature for which you want to set the tunables, and then click Set Tunables.
4. In the Set Signature Tunables panel, enter the new tunable values and click OK.
5. In the Result panel, verify that the operation was successful and click OK.

See “Viewing scan tunables associated with a policy scan” on page 310.

Set Signature Tunables options

Use this wizard panel to enter the new tunable values for the signature you selected. The tunable options that are displayed on this panel vary depending on the signature you have selected.

See “Setting signature tunables” on page 308.

Removing a signature from a policy template

In Veritas Operations Manager, you can remove a signature from a policy template under the Signatures tab in the policy template details. After you remove a signature from a policy template, it is not included in the future policy scans based on that policy template.

To remove a signature from a policy template

1. In the Veritas Operations Manager console, select Policies > Policy Templates.
2. Click on the desired policy template to view the policy template details.
3. On the Signatures tab, do one of the following:
   - Select the check box for the signature that you want to remove from the policy template and click Remove Signature.
Right-click the signature that you want to remove from the policy template, and then click **Remove Signature**.

4 In the **Remove Signature from Policy Template** panel, confirm that you want to remove the selected signature and click **Yes**.

5 In the **Result** panel, verify that the operation was successful and click **OK**.

See “About Installed Signatures” on page 299.
See “About policy templates” on page 290.
See “Adding signatures to a policy template” on page 308.

### Deleting a policy template scan

You can delete a policy check scan if you no longer require it.

**To delete a policy template scan**

1 In the console, select **Policies > Policy Templates**.

2 Click on the policy template to view the scan details.

3 Do one of the following:
   - Select the check box for the scan. Click **More** and select **Delete Scan**.
   - Right-click on the row for the scan to display the shortcut menu, and select **Delete Scan**.

4 In the **Delete Policy Template Scan** panel, confirm whether you want to delete the policy template scan.

5 In the **Result** panel, verify that the operation was successful and click **OK**.

See “About Policy Check” on page 290.
See “About policy templates” on page 290.
See “Running a manual policy template scan” on page 297.

### Viewing scan tunables associated with a policy scan

In Veritas Operations Manager, you can view the scan tunables that are associated with a policy scan under the **Scans** tab in the policy template details.
To view the scan tunables

1. In the Veritas Operations Manager console, select Policies > Policy Templates.
2. Click on the desired policy template to view the policy template details.
3. On the Scans tab, do one of the following:
   - Select the check box for the policy scan for which you want to view the associated tunables and then click More > Show Scan Tunables Used.
   - Right-click the policy scan for which you want to view the associated tunables, and then click Show Scan Tunables Used.

See “Setting signature tunables” on page 308.

Removing ignored violations from the ignore list

In Veritas Operations Manager, you can remove the ignored violations from the ignore list. After you remove the violations from the ignore list, they are listed in the scan details again.

To remove the ignored violations from the ignore list

1. In the Veritas Operations Manager console, select Policies > Policy Templates.
2. Click on the desired policy template to view the policy template details.
3. On the Ignored Violations tab, select the check boxes for the violations that you want to remove from the ignore list and do one of the following:
   - Click Remove from Ignore List.
   - Right-click one of the selected violations, and then click Remove from Ignore List.
4. In the Remove from Ignore List panel, confirm whether you want to remove the selected violations and click OK.
5. In the Result panel, verify that the operation was successful and click OK.

See “About policy violations” on page 298.

See “Marking policy violations to exclude from the subsequent scans” on page 298.
Removing ignored violations from the ignore list
Managing reports in Veritas Operations Manager

This chapter includes the following topics:

- About managing reports
- Running a report
- Creating a report schedule
- Editing a report schedule
- Enabling a report schedule
- Disabling a report schedule
- Removing a report schedule
- Archiving reports
- Sending a report through email
- Deleting an archived report
- Exporting report data to a file

About managing reports

In Veritas Operations Manager, you can perform the following tasks from the Reports view:

- Run a report.
- Schedule a report.
You must specify the business entities on which you want to run the report. If you want to run the report on all the business entities in the datacenter, you can select the **Entire Domain** option.

To schedule a report in Veritas Operations Manager, you must specify the following details:

- Scope of the report.
- Time and frequency at which you want to generate the report.
- Output types for the report that you schedule to generate.

In the report details view, you can perform the following tasks on the report schedules that you have created:

- Edit the report schedule.
- Enable the report schedule.
- Disable the report schedule.
- Delete the report schedule.

In any of the reports views in Veritas Operations Manager, you can do the following:

- Send the report details through email.
- Archive the report.

In the report details view, you can view the details of the reports that you have archived.

Also, you can perform the following tasks on the reports that you have archived:

- Delete an archived report.
- Send an archived report through email.

See “Running a report” on page 315.

See “Creating a report schedule” on page 316.

See “Editing a report schedule” on page 318.

See “Enabling a report schedule” on page 319.

See “Disabling a report schedule” on page 319.

See “Removing a report schedule” on page 319.

See “Archiving reports” on page 320.

See “Deleting an archived report” on page 323.

See “Sending a report through email” on page 321.
Running a report

You can run a report either from the Reports view or from the details view of a report.

To run a report

1  Do one of the following:
   ■  In the Reports view, identify the report that you want to generate and click Run.
   ■  In the details view of a report, click Run.

2  In the wizard panel to set the scope of the report, specify the scope and click Finish.

Select Scope options

Use this wizard panel to select the scope for running or scheduling a report. You can select the business entities that you need to include when you run or schedule a report.

Table 18-1  Select Scope options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Range</td>
<td>You can enter the following data to specify the date range for which you want to run the report.</td>
</tr>
<tr>
<td></td>
<td>■  In the Start Date field, enter the date on which the date range for the report starts.</td>
</tr>
<tr>
<td></td>
<td>■  In the End Date field, enter the date until which date range for the report lasts.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Date Range field appears for the reports that belong to the Trend/Activity category.</td>
</tr>
<tr>
<td>Entire Domain</td>
<td>Choose this option to include all the business entities when you run or schedule a report.</td>
</tr>
</tbody>
</table>
Creating a report schedule

You can create a report schedule so that the report is generated at the time and frequency that you specify.

You can schedule the report to run with the following frequency:

- Daily
- Weekly
- Monthly

In Veritas Operations Manager, business entities comprise application and organization entities.

To create a report schedule

1. Click **Reports** and do one of the following:
   - Identify the report that you want to schedule and click **Schedule**.
   - Click the name of the report that you want to schedule and in the detailed view of the report, click **Schedule**.

2. In the **Select Scope** wizard panel, enter the details and click **Next**.

3. In the **Schedule** wizard panel, enter the details and click **Next**.
   
   See “Schedule options” on page 317.

4. In the **Specify Schedule Details** wizard panel, enter the details and click **Next**.
   
   See “Specify Schedule Details options” on page 317.

5. In the **Summary** wizard panel, review the information and click **Finish**.

6. In the **Result** panel, click **OK**.
   
   See “Editing a report schedule” on page 318.

See “Removing a report schedule” on page 319.
Schedule options

Use this wizard panel to specify the recurrence of a report schedule.

### Table 18-2 Schedule options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Name</td>
<td>Enter the name of the schedule.</td>
</tr>
<tr>
<td>Date Range</td>
<td>You can enter the following data to specify the date range for which you want to schedule the report.</td>
</tr>
<tr>
<td></td>
<td>- In the <strong>Start Date</strong> field, enter the date on which you want to commence the report generation.</td>
</tr>
<tr>
<td></td>
<td>- In the <strong>End Date</strong> field, enter the date until which you want to generate the report.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Enter the frequency at which the reports are to be generated within the specified date range.</td>
</tr>
<tr>
<td></td>
<td>You can specify any of the following frequencies for a report:</td>
</tr>
<tr>
<td></td>
<td>- Daily</td>
</tr>
<tr>
<td></td>
<td>- Weekly</td>
</tr>
<tr>
<td></td>
<td>- Monthly</td>
</tr>
<tr>
<td>When</td>
<td>Specify the time at which the report is to be generated within the date range and frequency.</td>
</tr>
</tbody>
</table>

See “Creating a report schedule” on page 316.

See “Editing a report schedule” on page 318.

Specify Schedule Details options

Use this wizard panel to choose the output type for the report that you schedule.

This panel lets you choose one of the following output types:

- Email
- Archive.
### Table 18-3  Specify Schedule Details options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Choose this option if you want to send the report through email after it is generated based on the schedule that you create.</td>
</tr>
</tbody>
</table>
| Subject     | subject line of the report email.  
By default, the subject line is 'Emailing: Name of the report'. 
You can edit the subject line, if required. |
| To email address(s) | Enter one or more email addresses to which you want to send the report. Use ';' to separate the email addresses.                        |
| Archive     | Choose this option if you want to archive the report after it is generated based on the schedule that you create.                    |
| Archive File Name | Enter the file name in which the report is to be archived.                                                                               |

See “Creating a report schedule” on page 316.
See “Editing a report schedule” on page 318.

## Editing a report schedule

You can edit the details of a report schedule that you have created.

**Note:** In Veritas Operations Manager, business entities comprise application and organization entities.

To edit a report schedule

1. In the details view of a report, in the Schedules table, check the check box for the schedule that you want to modify and click **Edit**.
2. In the Select Scope wizard panel, modify the details, if required, and click **Next**
3. In the Schedule wizard panel, modify the details, if required, and click **Next**. 

See “Schedule options” on page 317.
4 In the Specify Schedule Details wizard panel, modify the details, if required, and click Next.

See “Specify Schedule Details options” on page 317.

5 In the Summary wizard panel, review the information that you have modified and click Finish.

6 In the Result panel, click OK.

See “Removing a report schedule” on page 319.

See “Creating a report schedule” on page 316.

Enabling a report schedule

You can enable a report schedule that you have created.

To enable a report schedule

1 In the details page of a report, in the Schedules table, check the check box for the report schedule that you want to enable and click Enable.

2 In the Enable Schedule panel, click Yes.

3 In the Results panel, click OK.

See “Disabling a report schedule” on page 319.

Disabling a report schedule

You can disable a report schedule that you have created.

To disable a report schedule

1 In the details page of a report, in the Schedules table, check the check box for the report schedule that you want to disable and click Disable.

2 In the Disable Schedule panel, click Yes.

3 In the Results panel, click OK.

See “Enabling a report schedule” on page 319.

Removing a report schedule

You can remove a report schedule that you have created.
To remove a report schedule

1. In the details page of a report, in the Schedules table, check the check box for the report schedule that you want to remove and click Delete.
2. In the Delete Schedule panel, click Yes.
3. In the Results panel, click OK.

See “Editing a report schedule” on page 318.
See “Creating a report schedule” on page 316.

Archiving reports

You can archive the contents of a report to view later or to email to other users. The data that is displayed in the archived report represents the state of the managed objects in the network at the time the report was created. For example, an operator can archive a report that shows the performance data at midnight and a system administrator can review the next morning.

Archived reports are stored on Management Server so that you and other users can display them in the console.

When you no longer need archived reports, you can delete them.

To archive a report

1. In the web console of the product, display a report.
2. In the top-right of the report, click Archive.
3. In the Archive Report wizard panel, enter the details and click OK.
   See “Archive Report Data options” on page 321.
4. In the Result panel, click OK.

To view an archived report

1. In the web console of the product, click Reports and identify the report for which you want to view the version of the report that you have archived earlier.
2. Click the name of the report.
3. In the details view of a report, in the Archived reports table, click the name of the report that you want to display in a new browser window.

The time and date at the top of the report identify when the archived report was created.
Archive Report Data options

Use this dialog box to create an archive of the report that is currently displayed. You can view the archived instances of a report in the Report Details view.

Table 18-4 Archive Report Data

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive File Name</td>
<td>Enter the name of the file for the archived report data. Veritas Operations Manager saves the archived reports in the HTML format. The file name should not contain any of the following characters: \/*?&quot;&lt;&gt;</td>
</tr>
</tbody>
</table>

See “Archiving reports” on page 320.

Sending a report through email

You can send a newly generated report through email. Also, you can send an archived report through email from the details view of the report.

Note: Before you send the report through email, you must define SMTP server, SMTP Port, and Sender Account in the SMTP Setting view.

To send a newly generated report through email

1. On the top-left of the window that displays the report, click Email.
2. In the Email Report Data wizard panel, enter the details and click Yes.
   
   See “Email Report Data options” on page 322.
3. In the Results panel, click OK.

To send an archived report through email

1. In the details view of a report, in the Archived reports table, check the check box for the report that you want to send through email and click Email.
2. In the Email Archived Report panel, enter the details and click Yes.
   
   See “Email Archived Report options” on page 322.
3. In the Results panel, click OK.

See “Deleting an archived report” on page 323.
See “Running a report” on page 315.

Email Archived Report options

Use this wizard panel to forward the selected archived report to an email recipient.

Table 18-5 Email Archived Report

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Name</td>
<td>Enter the name of your network’s SMTP server. Example: SMTPServer1.example.com</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter the subject of the email. Example: Archived Report from Friday</td>
</tr>
<tr>
<td>To email address(s)</td>
<td>Enter the email address of one or more recipients. Separate email addresses with a semicolon (;). Example: <a href="mailto:user1@example.com">user1@example.com</a>; <a href="mailto:user2@example.com">user2@example.com</a></td>
</tr>
<tr>
<td>From email address</td>
<td>Enter the sender’s email address. Example: <a href="mailto:user22@example.com">user22@example.com</a></td>
</tr>
</tbody>
</table>

See “Sending a report through email” on page 321.

Email Report Data options

Use this dialog box to send an HTML copy of the report data to one or more email recipients.

Table 18-6 Email Report Data

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Name</td>
<td>Enter the name of your network’s SMTP server. Maximum field length is 255 characters. Example: SMTPServer1.example.com</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter the subject of the email. Maximum field length is 255 characters. Example: Storage Allocation Summary Report</td>
</tr>
<tr>
<td>To email address(s)</td>
<td>Enter the email address of one or more recipients. Separate email addresses with a semicolon (;). Example: <a href="mailto:user1@example.com">user1@example.com</a>; <a href="mailto:user2@example.com">user2@example.com</a></td>
</tr>
</tbody>
</table>
Deleting an archived report

In the details view of a report, you can delete an archived report.

**To delete an archived report**

1. In the details view of a report, in the Archived reports table, check the check box for the archived report that you want to remove.
2. Click Delete.
3. In the Delete Archived Reports panel, click Yes.
4. In the Results panel to confirm the action, click OK.

See “Sending a report through email” on page 321.

Exporting report data to a file

When you export a report, the report data is captured on your computer in a comma-separated (.csv) file format. You can then open the file using either a spreadsheet program or a text editor.

**To preserve report data in a comma-separated file**

1. In the window that displays the report, do one of the following:
   - To export the summary part of a report to a .csv file, click Export at the top-right of the report window.
   - To export the data in the tables in a report to a .csv file, click the Save Table icon at the top-right of a table.
2. In the File Download dialog box, click Save.
3. In the Save As dialog box, specify the directory and the file name to which you want to save the data. and click Save.
Exporting report data to a file
Managing schedules in Veritas Operations Manager

This chapter includes the following topics:

■ About managing schedules in Veritas Operations Manager
■ Enabling schedules
■ Disabling schedules
■ Deleting schedules

About managing schedules in Veritas Operations Manager

In Veritas Operations Manager, you can view the various schedules that run in the system. The following are the two types of schedules that Veritas Operations Manager contains:

■ Schedules, which you can create using the Veritas Operations Manager console.
■ Preconfigured schedules, which are running on the managed hosts. These schedules are created when you added managed host to Veritas Operations Manager Management Server.

Note: You can create the schedules from the respective categories in Veritas Operations Manager.

You can view all the global schedules that are created on various events in Veritas Operations Manager in the Schedules view. Veritas Operations Manager lets you manage the schedules that you have created.
The security group and the associated business entity to which you belong decides the ownership of the schedule that you have created. Only the users who belong to the same security group can enable, disable, or remove the schedules.

In Veritas Operations Manager, the schedules belong to the following categories:

- Policy Check
- Licenses
- DR Fire Drill
- Report
- System
- Refresh Snapshot
- HA Fire Drill

In the Schedules view, you can perform the following tasks:

- Enable the schedules.
- Disable the schedules.
- Remove the schedules.

See “Enabling schedules” on page 326.
See “Disabling schedules” on page 327.
See “Deleting schedules” on page 327.

Enabling schedules

In Veritas Operations Manager, you can enable one or more schedules in the Schedules view.

To enable schedules

1. In the Veritas Operations Manager console, click Settings > Schedules.
2. In the Schedules view, check the check boxes for the schedules that you want to enable and click Enable.
3. In the Enable Schedule(s) panel, review the name and the recurrence information of the selected schedules and click Ok.
4. In the Result panel, click OK.

See “Disabling schedules” on page 327.
See “Deleting schedules” on page 327.
Disabling schedules

In Veritas Operations Manager, you can disable one or more schedules in the Schedules view.

To disable schedules

1. In the Veritas Operations Manager console, click **Settings > Schedules**.
2. In the **Schedules** view, check the check boxes for the schedules that you want to disable and click **Disable**.
3. In the **Disable Schedule(s)** panel, review the name and the recurrence information of the selected schedules and click **Ok**.
4. In the **Result** panel, click **OK**.

See “Disabling schedules” on page 327.

See “Deleting schedules” on page 327.

Deleting schedules

In Veritas Operations Manager, you can delete one or more schedules in the Schedules view.

To delete schedules

1. In the Veritas Operations Manager console, click **Settings > Schedules**.
2. In the **Schedules** view, check the check boxes for the schedules that you want to delete and click **Delete**.
3. In the **Delete Schedule(s)** panel, review the name and the recurrence information of the selected schedules and click **Ok**.
4. In the **Result** panel, click **OK**.

See “Enabling schedules” on page 326.

See “Disabling schedules” on page 327.
Managing Dynamic Multipathing paths in Veritas Operations Manager

This chapter includes the following topics:

- About using the Veritas DMP Maintenance functionality in Veritas Operations Manager
- Disabling the DMP paths on an array
- Disabling the DMP paths on an initiator
- Re-enabling the DMP paths on an array or initiator
- Resuming an incomplete DMP maintenance case
- Reviewing the output and results of a completed DMP maintenance case
- Removing a completed DMP maintenance case record

About using the Veritas DMP Maintenance functionality in Veritas Operations Manager

Dynamic Multipathing (DMP) lets you direct the communication to the storage through different sets of nodes to achieve failover and load balancing. When a connection fails, DMP spreads the communication to alternate paths automatically.

This release of Veritas Operations Manager provides you the options of disabling the DMP paths by choosing the arrays or the specific initiators in your datacenter.
In certain circumstances, you may want to perform maintenance operations on the array ports or on the initiators in your datacenter. For example, you may want to upgrade the firmware that has been installed on one or more initiators. In such situations, you may want to temporarily disable the DMP paths that connect these array ports and the initiators to the storage, and re-enable these paths after the maintenance operations are completed. When you temporarily disable the DMP paths that are connected to an array port or on an initiator, the communication to the storage is maintained through an alternate path.

Before you disable the DMP paths, you must ensure that the connected resources have alternate paths to the underlying physical storage. Veritas Operations Manager provides you options to verify the associated volumes, disk groups, hosts, and applications that currently use the storage that is connected through the selected initiators or array ports.

The following table lists the user privileges that are required for performing the DMP maintenance operation.

<table>
<thead>
<tr>
<th>User role</th>
<th>Actions allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Admin</td>
<td>Can manage all resources in the domain. The domain admin user can complete the maintenance cases that were started by an admin, domain operator, or an operator.</td>
</tr>
<tr>
<td>Admin with storage access</td>
<td>Allowed to perform DMP maintenance on the arrays and the initiators that are connected to hosts on which they have admin access.</td>
</tr>
<tr>
<td>Admin without storage access</td>
<td>Allowed to perform DMP maintenance only on the initiators that are connected to hosts on which they have admin access.</td>
</tr>
</tbody>
</table>

*Note*: You cannot use the Veritas Operations Manager to manage the DMP paths for Windows managed hosts.

**Disabling the DMP paths on an array**

In certain circumstances, you may want to perform maintenance operations on the array ports or array adapters in your datacenter. For example, you may want to upgrade the firmware that has been installed on the array adapter. In such a situation, you may want to temporarily disable the DMP paths that connect this array adapter to the storage, and re-enable these paths after the maintenance
operations are completed. When you temporarily disable the DMP paths on an array port or an array adapter, the communication to the storage is maintained through an alternative path.

Veritas Operations Manager lets you disable the DMP paths by choosing specific arrays in your datacenter.

**To disable the DMP paths on an array**

1. In the Veritas Operations Manager console, do one of the following:
   - Select **Solutions** to go the Solutions page. Under **Veritas DMP Maintenance**, click **Start new Veritas DMP Maintenance case**.
   - Select **Manage > Enclosures**. In the Enclosures list page, select an enclosure and click **Veritas DMP Maintenance**.

2. In the **Start** panel, ensure that **Array** is selected, and enter the required information. Click **Next**.
   
   See “**Start panel options**” on page 332.

3. In the **Select Enclosure** wizard panel, choose the enclosure that contains the array port or the array adapter on which you want to perform maintenance. Click **Next**.
   
   See “**Select Enclosure panel options**” on page 333.

4. In the **Specify Array Port(s)** wizard panel, choose the array port or the array adapter that contains the ports on which you want to perform maintenance. You can choose from array adapters only if the Veritas Operations Manager Storage Insight Add-on is configured for the selected array.
   
   See “**Specify Array Port(s) panel options**” on page 334.

5. In the **Path Disable Confirmation** panel, review the details of the DMP paths. To view the information on the relationship of the DMP paths with other resources in your datacenter, click **View Associations Report**.
   
   See “**Path Disable Confirmation panel options**” on page 334.
   
   See “**Veritas DMP Maintenance Associations Report**” on page 335.

6. In the **Path Disable Confirmation** panel, click **Disable** to disable all the listed DMP paths.
   
   See “**Path Disable Confirmation panel options**” on page 334.

7. In the **Paths Disabled** panel, review the details of the disabled paths and the commands that were run to complete the operation. Do one of the following:
   
   - To save and close the configuration and re-enable the DMP paths later, click **Save&Close**. If you choose this option, you can re-enable the DMP
paths later using the options available on the **Solutions** page, or using the **Unfinished Cases** drop-down in the **Start** wizard panel.

- To re-enable the DMP paths after the array port or the array adapter maintenance operations are completed, click **Next**.

See “**Paths Disabled panel options**” on page 336.

### Start panel options

Use this wizard panel to start a new Dynamic Multipathing (DMP) maintenance case or resume a partially completed DMP maintenance case.

This panel lets you specify a name for a new DMP maintenance case that you want to start. You can use this name to refer to the DMP maintenance case with this name later on.

You can resume an incomplete DMP maintenance case by selecting the case name in this panel.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start New Veritas DMP Maintenance Case</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Maintenance Type</strong></td>
<td>Lets you select the storage object to perform the DMP maintenance operation. Choose:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Array</strong> to disable the DMP paths to perform maintenance on an array port, or an array adapter (if the Veritas Operations Manager Storage Insight Add-on is configured for the array).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Initiator</strong> to disable the DMP paths to perform maintenance on an initiator.</td>
</tr>
<tr>
<td><strong>Case Name</strong></td>
<td>Name of the new DMP maintenance case that you want to start. You can use this name to refer to the case later on.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>The additional information that you want to include for the new DMP maintenance case. This field is optional.</td>
</tr>
</tbody>
</table>

**Resume Existing Veritas DMP Maintenance Case**
Table 20-1 Start panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unfinished Cases</td>
<td>From the drop-down list, select the incomplete DMP maintenance case that you want to complete.</td>
</tr>
</tbody>
</table>

See “Disabling the DMP paths on an array” on page 330.

See “Disabling the DMP paths on an initiator” on page 336.

Select Enclosure panel options

Use this wizard panel to select the enclosure that contains the array ports on which you want to perform maintenance operations.

This panel lists the enclosures available in Veritas Operations Manager that have Veritas DMP configured on exported LUNs. It does not list the enclosures that do not use DMP. To filter the list, enter the keywords, such as the first few letters of the enclosure name, in the Filter field.

Select the enclosure that contains the array ports on which you want to perform maintenance operations. When you select the option, the row that represents the enclosure is highlighted.

Table 20-2 Select Enclosure panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the disk enclosure</td>
</tr>
<tr>
<td>Serial</td>
<td>Serial number of the disk enclosure</td>
</tr>
<tr>
<td>Vendor</td>
<td>Name of the manufacturer of the disk enclosure</td>
</tr>
<tr>
<td>Product</td>
<td>Name of the array model</td>
</tr>
<tr>
<td>Type</td>
<td>Type of array</td>
</tr>
<tr>
<td>Total Objects</td>
<td>Total number of the disk enclosures that are listed on the panel</td>
</tr>
</tbody>
</table>

See “Disabling the DMP paths on an array” on page 330.
Specify Array Port(s) panel options

Use this wizard panel to select the array ports on which you want to disable the associated DMP paths. You can also use this wizard to clear the paths that you do not want to disable.

This panel displays the names of the array ports and their Array Port WWN. Select one or more array ports on which you want to disable the associated DMP paths. To filter the list, enter the keywords (preferably, the first few letters of the enclosure) in the Filter field.

By default, when you select an array port, all the paths that are associated with that array port are also selected.

You cannot select any non-redundant paths that are associated with an array port. Single paths are highlighted in red.

See “Disabling the DMP paths on an array” on page 330.

See “Disabling the DMP paths on an initiator” on page 336.

Path Disable Confirmation panel options

Use this wizard panel to view the details of the DMP paths that you have selected for disabling.

You can click the View Association Report link to view the information on the relationship of the DMP paths that you want to disable with other storage resources.

Table 20-3 Path Disable Confirmation panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Names of the DMP paths that you have selected for disabling</td>
</tr>
<tr>
<td>Status</td>
<td>Current status of the DMP Paths that you have selected for disabling</td>
</tr>
<tr>
<td>Devices</td>
<td>Name of the disk where the path is located</td>
</tr>
<tr>
<td>Active Paths</td>
<td>The number of the active DMP paths</td>
</tr>
<tr>
<td>Host</td>
<td>Host to which the DMP Paths that you have selected for disabling is connected</td>
</tr>
<tr>
<td>Initiator</td>
<td>Initiator to which the DMP path is associated</td>
</tr>
</tbody>
</table>
Table 20-4 Veritas DMP Maintenance Associations Report fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Enclosure</td>
<td>Name of the enclosure that contains the array ports to which the DMP paths that you want to disable are associated. If you are performing the DMP maintenance on an initiator, the selected enclosure is not displayed in this report.</td>
</tr>
<tr>
<td>Case Name</td>
<td>Name of the DMP maintenance case that you entered</td>
</tr>
<tr>
<td>Associations for Array Port</td>
<td>Selected array port on which you want to disable the DMP paths</td>
</tr>
<tr>
<td>Business Entities</td>
<td>The details of the business entities that are associated with the selection</td>
</tr>
<tr>
<td>Hosts</td>
<td>The details of the hosts that are associated with the selection</td>
</tr>
<tr>
<td>Volumes</td>
<td>The details of the volumes that are associated with the selection</td>
</tr>
</tbody>
</table>
Table 20-4  Veritas DMP Maintenance Associations Report fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disks</td>
<td>The details of the disks that are associated with the selection</td>
</tr>
</tbody>
</table>

See “Disabling the DMP paths on an array” on page 330.

Paths Disabled panel options

Use this wizard panel to view the output summary of the DMP path disabling operation. This wizard panel displays the following information:

Table 20-5  Path Disabled panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Path Disable Operation Output Summary |  ■ Total number of successful commands.  
  ■ Total number of failed DMP commands.  |
| Command Details                 | ■ Hosts on which the successful DMP commands were run  
  ■ Details of the DMP paths that are disabled  
  ■ Details of the failed DMP commands and the reason for the failure. |

See “Disabling the DMP paths on an array” on page 330.

See “Disabling the DMP paths on an initiator” on page 336.

Disabling the DMP paths on an initiator

In certain circumstances, you may want to perform maintenance operations on the initiators in your datacenter. For example, you may want to upgrade the firmware that has been installed on one or more initiators. In such situations, you may want to temporarily disable the Dynamic Multipathing (DMP) paths that connect these initiators to the storage, and re-enable these paths after the maintenance operations are completed. When you temporarily disable the DMP paths on an initiator, the communication to the storage is maintained through an alternative path.

Veritas Operations Manager lets you disable the DMP paths by choosing specific initiators.
To disable the DMP paths on an initiator

1. In the Veritas Operations Manager console, do one of the following:
   - Select Solutions to go the Solutions page. Under Veritas DMP Maintenance, click Start new Veritas DMP Maintenance case.
   - Select Manage > Hosts. In the Hosts list page, click on a host, and click Initiator. Select the required initiator, and click Veritas DMP Maintenance.

2. In the Start panel, and enter the required information. Click Next.
   See “Start panel options” on page 332.

3. In the Select Host(s) panel, select one or more hosts that contain the initiator. Click Next
   See “Select Host(s) panel options” on page 338.

4. In the Select Initiators panel, select one or more initiators that contain the DMP paths that you want to disable.
   See “Select Initiators panel options” on page 338.

5. In the Path Disable Confirmation panel, review the details of the DMP paths. To view the information on the relationship of the DMP paths with other storage resources in your datacenter, click View Associations Report.
   See “Path Disable Confirmation panel options” on page 334.
   See “Veritas DMP Maintenance Associations Report” on page 335.

6. In the Path Disable Confirmation panel, click Disable to disable all the listed DMP paths.
   See “Path Disable Confirmation panel options” on page 334.

7. In the Paths Disabled panel, review the details of the disabled paths and the commands that were run to complete the operation. Do one of the following:
   - To save and close the configuration and re-enable the DMP paths later, click Save&Close. If you choose this option, you can re-enable the DMP paths later using the options available on the Solutions page, or using the Unfinished Cases drop-down in the Start wizard panel.
   - To re-enable the DMP paths after the array or the array adapter maintenance operations are completed, click Next.
   See “Paths Disabled panel options” on page 336.
Select Host(s) panel options

Use this wizard panel to select the hosts that contain the initiators on which you want to perform maintenance.

You can enter the keywords, such as the first few letters of the host name, in the **Filter** field to filter the list. You can filter this list by the name of the host, the IP address, the architecture of the host, or by the platform the host runs.

**Note:** You cannot use the Veritas Operations Manager to manage the DMP paths for Windows managed hosts.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the host</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the host</td>
</tr>
<tr>
<td>Architecture</td>
<td>The architecture of the host, such as PowerPC and SPARC</td>
</tr>
<tr>
<td>Platform</td>
<td>The operating system that the host uses</td>
</tr>
</tbody>
</table>

See “Disabling the DMP paths on an initiator” on page 336.

Select Initiators panel options

Use this wizard panel to select the initiators to perform maintenance by disabling the Dynamic Multipathing (DMP) paths. You can select multiple initiators from this list at a time.

You can enter the keywords, such as the first few letters of the initiator name, in the **Filter** fields to filter the list. You can filter this list by the name of the initiator, the version of the driver, version of the firmware, or by the name of the vendor.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the initiator</td>
</tr>
<tr>
<td>Host</td>
<td>The host to which the initiator is associated</td>
</tr>
<tr>
<td>Driver Version</td>
<td>The version of the driver for the initiator</td>
</tr>
</tbody>
</table>
### Table 20-7 Select Initiators panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Version</td>
<td>The version of the firmware that is used on the initiator</td>
</tr>
<tr>
<td>Vendor</td>
<td>The manufacturer of the initiator</td>
</tr>
</tbody>
</table>

See “Disabling the DMP paths on an initiator” on page 336.

## Re-enabling the DMP paths on an array or initiator

In Veritas Operations Manager, you can re-enable the DMP paths that you have disabled as part of the maintenance operation. You can re-enable the DMP paths in the following ways:

- Immediately after disabling the DMP paths for an array port, array adapter, or an initiator
- Using the [Total number of waiting cases] case(s) waiting for user action link on the Solutions page
- Using the wizard panel to start a new DMP maintenance case

### Re-enabling the DMP paths immediately after disabling them

1. After you disable the DMP paths on an array or an initiator, click **Next**.
   See “Paths Disabled panel options” on page 336.

2. In the **Paths Re-Enable Confirmation** panel, click **Re-Enable**.
   See “Paths Re-Enable Confirmation panel options” on page 341.

3. In the **Paths Enabled** panel, review the details of the re-enabled paths. Click **Next**.
   See “Paths Enabled panel options” on page 341.

4. In the **Veritas DMP Maintenance Result Summary** page, view the details of the current paths and the commands run to complete the operation. Click **Close**.
   See “Veritas DMP Maintenance Result Summary” on page 342.
Re-enabling the DMP paths using the Solutions home page option

1. In the Veritas Operations Manager console, select **Solutions** to go the Solutions page.

2. Under **Veritas DMP Maintenance**, click the link for the cases pending for the user action.

3. In the **Veritas DMP Maintenance Waiting Cases** page, select the pending case and click **Resume Case and Re-Enable Paths**

4. In the **Paths Re-Enable Confirmation** panel, click **Re-Enable**.
   See “**Paths Re-Enable Confirmation panel options**” on page 341.

5. In the **Paths Enabled** panel, review the details of the re-enabled paths. Click **Next**.
   See “**Paths Enabled panel options**” on page 341.

6. In the **Veritas DMP Maintenance Result Summary** page, view the details of the current paths and the commands run to complete the operation. Click **Close**.
   See “**Veritas DMP Maintenance Result Summary**” on page 342.

Re-enabling the DMP paths using the Start wizard panel

1. In the Veritas Operations Manager console, select **Solutions** to go the Solutions page.

2. Under **Veritas DMP Maintenance**, click **Start new Veritas DMP Maintenance case**.

3. In the **Start** panel, click **Resume Existing Veritas DMP Maintenance Case** and choose a case name from the **Unfinished Cases** drop-down list. Click **Next**.
   See “**Start panel options**” on page 332.

4. In the **Paths Re-Enable Confirmation** panel, click **Re-Enable**.
   See “**Paths Re-Enable Confirmation panel options**” on page 341.

5. In the **Paths Enabled** panel, review the details of the re-enabled paths. Click **Next**.
   See “**Paths Enabled panel options**” on page 341.

6. In the **Veritas DMP Maintenance Result Summary** page, view the details of the current paths and the commands run to complete the operation. Click **Close**.
   See “**Veritas DMP Maintenance Result Summary**” on page 342.
Paths Re-Enable Confirmation panel options

Use this wizard panel to view the details of the DMP paths that you want to re-enable after performing maintenance on the associated storage resource. These DMP paths were disabled before you performed maintenance.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the DMP paths that you want to re-enable</td>
</tr>
<tr>
<td>Device</td>
<td>Disk device to which the DMP path is associated</td>
</tr>
<tr>
<td>Host</td>
<td>Host to which the DMP path is associated</td>
</tr>
<tr>
<td>Initiator</td>
<td>Initiator to which the DMP path is associated</td>
</tr>
<tr>
<td>Array Port</td>
<td>Array port to which the DMP Paths that you want to re-enable is associated</td>
</tr>
</tbody>
</table>

See “Re-enabling the DMP paths on an array or initiator” on page 339.

Paths Enabled panel options

Use this wizard panel to view the output summary of the path re-enable operation. On this panel, you can view the following:

- Details of the path re-enable commands that successfully executed
- DMP paths that are re-enabled
- Hosts on which the commands that successfully disabled the DMP paths are executed
- Commands that failed to re-enable the DMP paths, if any

This panel displays the name of the DMP maintenance case that you are currently processing. It also displays the name of the enclosure that contains the array ports with which the DMP paths that you are re-enabling are associated.

Under Path Enable Operation Output Summary, you can view the path enable commands that are successfully executed. You can also view the path enable commands that are failed along with the output details.

Under Command Details, you can view the details of the path enable commands that successfully executed and the path enable commands that failed. For the successful path enable commands, this panel displays the DMP paths that are
enabled and the host with which these paths are associated. You can also view the details of the path enable commands that failed, if any.

See “Re-enabling the DMP paths on an array or initiator” on page 339.

Veritas DMP Maintenance Result Summary

Use this wizard panel to view the overall summary of the Dynamic Multipathing (DMP) maintenance case that you have completed.

This panel lists the following details:

- DMP paths that were managed and their current statuses
- All commands that are executed during the DMP maintenance operation and their results

Table 20-9  Veritas DMP Maintenance Result Summary panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current Path Status</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the DMP path on which you have completed the state management</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the DMP path</td>
</tr>
<tr>
<td>Device</td>
<td>The disk device to which the DMP path is associated</td>
</tr>
<tr>
<td>Host</td>
<td>Host to which the DMP path is associated</td>
</tr>
<tr>
<td>Initiator</td>
<td>The initiator to which the DMP path is associated</td>
</tr>
<tr>
<td>Array Port</td>
<td>Array port to which the DMP path is associated</td>
</tr>
<tr>
<td><strong>All Commands Executed and Results</strong></td>
<td></td>
</tr>
<tr>
<td>Disable Path Commands Executed</td>
<td>Displays the names of the commands that are run for disabling the DMP paths with the name of the host on which they were run</td>
</tr>
<tr>
<td>Enable Path Commands Executed</td>
<td>Displays the name of the commands that are run for enabling the DMP paths with the name of the host on which they were run</td>
</tr>
</tbody>
</table>

See “Disabling the DMP paths on an array” on page 330.
Resuming an incomplete DMP maintenance case

Using Veritas Operations Manager, you can disable the Dynamic Multipathing (DMP) paths in your datacenter before you perform the maintenance of the array ports or the initiators. After the maintenance operations are completed, you can re-enable the DMP paths that are connected to the arrays and initiators. Veritas Operations Manager provides you options for re-enabling the DMP paths using the same wizard panel that you used for disabling the DMP paths. However, if you want to save and close the configuration after the disabling operation is complete, you can re-enable the DMP paths from the [Total number of waiting cases] case(s) waiting for user action link on the Solutions home page.

To resume an incomplete DMP maintenance case

1. In the Veritas Operations Manager console, select Solutions to go the Solutions page.

2. In the Solutions page, under Veritas DMP Maintenance, click the [Total number of waiting cases] case(s) waiting for user action link.

3. In the DMP Maintenance Waiting Cases page, under Waiting Cases, select the incomplete DMP maintenance case that you want to resume. Click Resume Case and Re-enable Paths.

4. In the Paths Re-Enable Confirmation panel, click Re-Enable.

   See “Paths Re-Enable Confirmation panel options” on page 341.

5. In the Paths Enabled panel, review the details of the re-enabled paths. Click Next.

   See “Paths Enabled panel options” on page 341.

6. In the Veritas DMP Maintenance Result Summary page, view the details of the current paths and the commands run to complete the operation. Click Close.

   See “Veritas DMP Maintenance Result Summary” on page 342.
Reviewing the output and results of a completed DMP maintenance case

Using the Veritas Operations Manager console, you can view the status of the DMP path and the list of commands that were run as part of the DMP maintenance process.

You can view these details in the following two ways:

- Immediately after the process of re-enabling the DMP paths after the maintenance operations are completed on the array ports or the host bus adapters
- Using the Veritas DMP Maintenance Completed Cases page

This topic describes how you can view the output and the results of a completed DMP maintenance case using the Veritas DMP Maintenance Completed Cases page.

To review the output and the results of a completed DMP maintenance case

1. In the Veritas Operations Manager console, select Solutions to go the Solutions page.
2. In the Solutions page, under Veritas DMP Maintenance, click the [Total number of] case(s) completed link.
3. In the Veritas DMP Maintenance Completed Cases page, under Completed Cases, select the completed DMP maintenance cases that you want to remove. Click Show Case Output and Results.
4. In the Veritas DMP maintenance Result Summary page, review the information.

See “Veritas DMP Maintenance Result Summary” on page 342.

See “Disabling the DMP paths on an array” on page 330.

See “Disabling the DMP paths on an initiator” on page 336.

Removing a completed DMP maintenance case record

The Veritas Operations Manager database keeps the records of each of the completed DMP maintenance cases. If you do not want to keep this record for a longer period of time, you can remove them from the database using the Veritas Operations Manager console.
To remove a completed DMP maintenance case record

1. In the Veritas Operations Manager console, select **Solutions** to go to the Solutions page.

2. In the Solutions page, under **Veritas DMP Maintenance**, click the **[Total number of] case(s) completed** link.

3. In the **Veritas DMP Maintenance Completed Cases** page, under **Completed Cases**, select the completed DMP maintenance cases that you want to remove. Click **Delete Cases**.

4. In the **Delete Completed Case** confirmation panel, click **Yes**.
Removing a completed DMP maintenance case record
Managing extended attributes on storage objects in Veritas Operations Manager

This chapter includes the following topics:

- About using extended attributes on the objects in Veritas Operations Manager
- Viewing the list of extended attributes in Veritas Operations Manager
- Defining an extended attribute on one or more storage objects
- Modifying an extended attribute in Veritas Operations Manager
- Removing an extended attribute in Veritas Operations Manager
- Setting values to the extended attributes on one or more objects
- Modifying the extended attributes value on an object

About using extended attributes on the objects in Veritas Operations Manager

An extended attribute is an additional user-defined attribute that provides additional details about an object in Veritas Operations Manager. This information about an object is in addition to the details that Veritas Operations Manager discovers for that object. You can define multiple extended attributes on Veritas
Managing extended attributes on storage objects in Veritas Operations Manager

Operations Manager objects. You can use the extended attributes to search, filter, and sort the objects in Veritas Operations Manager.

You can define an extended attribute in Veritas Operations Manager and associate it with the relevant objects. You need to set the value for the extended attribute when you associate it with the object. Also, you can associate an extended attribute with the base object type of a business entity. When you associate the extended attributes with a business entity, it applies the values for the extended attributes to all the objects that are part of the base object type of the business entity.

In Veritas Operations Manager, you can define the extended attributes only for the following object types:

- Host
- File System
- Disk group
- Enclosure
- Databases
- Exchange Server
- Cluster
- Service Group
- LUN

See “Defining an extended attribute on one or more storage objects” on page 349.

See “Viewing the list of extended attributes in Veritas Operations Manager” on page 348.

Viewing the list of extended attributes in Veritas Operations Manager

In Veritas Operations Manager, the **Extended Attributes** view lists all the extended attributes that you have defined, in a table.

In the table that list the extended attributes, you can view the following details:

- Unique name of the extended attribute that you have defined.
- Object type that is associated with the extended attribute.
- Whether you want to display the extended attribute as a column in the object views.

You can sort the table based on the **Attributes Name** column.
You can use the free text search box on the left side panel to filter the table that lists the extended attributes. Also, you can use the options under the **Object Type** heading to filter the Extended Attributes table.

In the Extended Attributes view, you can perform the following tasks:

- Defining an extended attribute.
- Modifying an existing extended attribute.
- Removing an extended attribute.

**To view the list of extended attributes in Veritas Operations Manager**

- In the Veritas Operations Manager console, select **Settings > Extended Attributes**.

See “Defining an extended attribute on one or more storage objects” on page 349.

See “Modifying an extended attribute in Veritas Operations Manager” on page 351.

See “Removing an extended attribute in Veritas Operations Manager” on page 352.

See “About using extended attributes on the objects in Veritas Operations Manager” on page 347.

### Defining an extended attribute on one or more storage objects

In the **Extended Attributes** view, Veritas Operations Manager lets you define one or more extended attributes for multiple object types. You can define only the names of the extended attributes. Also, you can specify whether the extended attribute that you have defined should appear as a column in the relevant object view. Otherwise, the extended attribute that you have defined appears in the details view of the object. It also appears as a hidden column in the **Table Settings** dialog box of the table in which the object is listed in Veritas Operations Manager. You can use the value that you have defined for the extended attribute to search, filter, or sort the objects in the view.

**Note:** Only the users with the Domain Admin role can define an extended attribute for an object type.

The extended attributes that you define for an object type apply to all the objects that are part of the object type. After you define an extended attribute on an object type, other users with Administrator, Domain Operator, or Operator roles can set the values for the extended attribute in the relevant views.
For example, you can define the extended attribute named **Location** on the Hosts object type. All the hosts in the domain display this extended attribute. The Administrator who knows that a specific host that is located in New York can set the value for the location attribute for that host as **New York**. In the host view, the **Location** column for that host displays the value as **New York**.

**To define an extended attribute on one or more storage objects**

1. In the Veritas Operations Manager console, select **Settings > Extended Attributes**.
2. In the **Extended Attributes** view, click **Define**.
3. In the **Define Extended Attribute** wizard panel, enter the required data and click **OK**.
   See “Define Extended Attribute options” on page 350.
4. In the **Results** panel that confirms that the extended attribute is successfully created, click **OK**.
   See “Modifying an extended attribute in Veritas Operations Manager” on page 351.
   See “Removing an extended attribute in Veritas Operations Manager” on page 352.
   See “Viewing the list of extended attributes in Veritas Operations Manager” on page 348.
   See “Viewing the list of extended attributes in Veritas Operations Manager” on page 348.

**Define Extended Attribute options**

Use this wizard panel to define the extended attribute for one or more object types.

**Table 21-1** Define Extended Attribute panel options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the extended attribute. Veritas Operations Manager uses the name that you enter in this field to identify the extended attribute that you define. <strong>Note:</strong> Ensure that the name that you provide to the extended attribute is not used for any of the existing attributes of the object types.</td>
</tr>
</tbody>
</table>
Table 21-1  Define Extended Attribute panel options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Object Type** | Select one of the following object types for which you can define the extended attribute:  
  - Host  
  - File System  
  - Disk group  
  - Enclosure  
  - Databases  
  - Exchange Server  
  - Cluster  
  - Service Group  
  - LUN |
| **Show as Column** | Select this checkbox against each object type to display the extended attribute as a column in the relevant object views or as an optional column in the Table Settings of table in which the object type is listed in Veritas Operations Manager. If you have not selected this check box, you can view the extended attribute in the details view of the object. |

See “Defining an extended attribute on one or more storage objects” on page 349.

Modifying an extended attribute in Veritas Operations Manager

In the Extended Attributes view, Veritas Operations Manager lets you modify the name of the extended attributes that you have defined.

**Note:** Only the users with the Domain Admin role can modify an extended attribute.

When you modify the name of the extended attribute, Veritas Operations Manager ensures that the updated name is unique in the domain. Then, Veritas Operations Manager updates the objects to display the new name for the extended attribute. Also, you can set a different value for the modified external attribute in the object views. In this way, modifying an extended attribute is equivalent to defining a new extended attribute.
To modify an extended attribute in Veritas Operations Manager

1. In the Veritas Operations Manager console, select **Settings > Extended Attributes**.

2. In the **Extended Attributes** view, select the extended attribute that you want to modify and click **Modify**.

3. In the **Edit Extended Attribute** wizard panel, modify the name of the extended attribute and click **OK**.
   See “Edit Extended Attribute options” on page 352.

4. In the **Results** panel that confirms that the extended attribute is successfully modified, click **OK**.
   See “Defining an extended attribute on one or more storage objects” on page 349.
   See “Viewing the list of extended attributes in Veritas Operations Manager” on page 348.

### Edit Extended Attribute options

Use this panel to modify the name of an extended attribute that you have defined.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object Type</strong></td>
<td>Displays the name of the object type that you have specified for the extended attribute. You cannot modify this field.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter the new name of the extended attribute.</td>
</tr>
</tbody>
</table>

See “Modifying an extended attribute in Veritas Operations Manager” on page 351.

### Removing an extended attribute in Veritas Operations Manager

In the **Extended Attributes** view, Veritas Operations Manager lets you remove an extended attribute that you have defined. When you remove an extended attribute, its association with the objects are also removed. Therefore, these extended attributes are not visible in the relevant object’s views.

**Note:** Only the users with the Domain Admin role can modify an extended attribute.
To remove an extended attribute in Veritas Operations Manager

1. In the Veritas Operations Manager console, select **Settings > Extended Attributes**.

2. In the **Extended Attributes** view, select the extended attribute that you want to remove and click **Delete**.

3. In the **Delete Extended Attribute** wizard panel, click **Yes**.

4. In the **Result** panel that confirms that the extended attribute is successfully removed, click **OK**.

See “Defining an extended attribute on one or more storage objects” on page 349.
See “Modifying an extended attribute in Veritas Operations Manager” on page 351.

Setting values to the extended attributes on one or more objects

Veritas Operations Manager lets you set the values for the extended attributes that are defined for a specific object. You can set the values for the extended attributes from the relevant object views.

**Note:** Users with the Domain Admin, Admin, Domain Operator, and Operator roles can set the values for an extended attribute.

If you want to set the values for the extended attributes of multiple objects, you must select the objects in the relevant object views before you perform this task. For example, if you want to set the value for the extended attribute named **Location** on multiple hosts, you must select those hosts in the **Hosts** view before you perform this task.

To set values to the extended attributes on one or more objects

1. In the Veritas Operations Manager console, navigate to the relevant object view.

2. In the object view, in the table that lists the objects, select the check box on the left side of one or more objects on which you want to set the value for the extended attributes.

3. Do one of the following:
   - At the top of the objects view table, click **Set Extended Attributes**.
   - Right-click the highlighted rows in the table that represent the object that you have selected. From the sub menu, select **Set Extended Attributes**.
4 In the **Set Extended Attributes** panel, select the check box on the left side of the name of the attribute.

See “**Set Extended Attributes option**” on page 354.

5 In the **Value** field, enter the value for the attribute and click **OK**.

See “**Defining an extended attribute on one or more storage objects**” on page 349.

See “**Modifying the extended attributes value on an object**” on page 354.

See “**Setting the extended attributes on a business entity**” on page 211.

### Set Extended Attributes option

Use this panel to specify the values for the extended attributes on the objects that you have selected in the objects table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the extended attribute that you have defined for the object.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter the value that you want to specify for the extended attribute.</td>
</tr>
</tbody>
</table>

See “**Setting values to the extended attributes on one or more objects**” on page 353.

### Modifying the extended attributes value on an object

Veritas Operations Manager lets you modify the values that you have set for the extended attributes defined for a specific object. You can modify the values for the extended attributes from the details view of the relevant object.

**To modify the values that are set for the extended attributes on an object**

1 In the Veritas Operations Manager console, navigate to the relevant object view.

2 In the object view, in the table that lists the objects, click the name of the object to navigate to its details view.
3 In the details view of the object, on the task toolbar, select **Environment > Edit Extended Attributes**.

4 In the **Edit Extended Attributes** wizard panel, modify the extended attribute value and click **OK**.

See “**Edit Extended Attributes option (object)**” on page 355.

See “**Setting values to the extended attributes on one or more objects**” on page 353.

See “**Setting the extended attributes on a business entity**” on page 211.

### Edit Extended Attributes option (object)

Use this panel to modify the values that you have set for the extended attributes on a relevant object.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the extended attribute that you have defined for the object.</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the existing value for the extended attribute. You can modify the value that is already specified in this field.</td>
</tr>
</tbody>
</table>

See “**Modifying the extended attributes value on an object**” on page 354.
This appendix includes the following topics:

- sfmw
- vomsc
- vxlist
- xdistc
sfmw


SYNOPSIS

sfmw start | stop | restart | status | listports

DESCRIPTION

sfmw starts and stops the Tomcat Web server, the Veritas Operations Manager Web application, and the Storage Management (SM) Web application

KEYWORDS

start

Starts the Tomcat Web server, the Veritas Operations Manager Web application, and the Storage Management (SM) Web application, if not already running.

stop

Terminates the Veritas Operations Manager Web application, Storage Management (SM) Web application (if already running), and the Tomcat Web server.

restart

Stops the Veritas Operations Manager Web application, the Storage Management (SM) Web Application (if already running), and the Tomcat Web server, then starts them.

status

Indicates whether the Veritas Operations Manager Web application is running.

listports

Displays the HTTPS port that the Tomcat Web server listens to for connections.

NOTES

On UNIX, the default installation path is: /opt/VRTSsfmcs/cweb

The log for Veritas Operations Manager and the SM Web application resides by default in: /var/opt/VRTSsfmcs/esmweb/log
vomsc

vomsc - enables you to manage Veritas Operations Manager services on a UNIX-based Management Server.

SYNOPSIS

vomsc {start | stop | status | version} {service | ALL}

DESCRIPTION

The vomsc script lets you start or stop one or more Veritas Operations Manager services on a UNIX-based Management Server. You can also use the script to check the status of one or more services. The change in the state of the services is temporary. When the host is restarted, all the services are started again.

You can use the vomsc script to view the version of the VRTSsfmcs package and the VRTSsfmh package that is installed on the Management Server host.

The vomsc script is not supported in the HA environment.

KEYWORDS

start
   Starts the specified service, or all the services that the script manages.

stop
   Stops the specified service, or all the services that the script manages.

status
   Displays the status of the specified service, or all the services that the script manages.

version
   Displays the version of the VRTSsfmcs package and the VRTSsfmh package that is installed on the Management Server host.

service
   The services managed by the vomsc script that you can specify are:
   - xprtld - Veritas Operations Manager Messaging Service
   - sfmh-discovery - Veritas Operations Manager watchdog
   - vxdcli - Foundation Distributed Command Line Daemon
   - vxsfmcsdb - Veritas Operations Manager Database Service
- sfmsecd - Veritas Operations Manager Security Service
- sfmcswd - Veritas Operations Manager Web console

ALL
Performs the operation on all the services that the script manages.

EXAMPLES

This section provides usage examples for `vomsc`.

EXAMPLE 1:
To start the `xprtld` service.

```
vomsc start xprtld
```

EXAMPLE 2:
To stop all the Veritas Operations Manager services that the `vomsc` script manages.

```
vomsc stop ALL
```

EXAMPLE 3:
To display the status of the database service.

```
vomsc status vxsfmcsdb
```

NOTES

The default location of `vomsc` on UNIX is `/opt/VRTSsfmcs/bin/`.

On Windows, you can use the `C:\Program Files\Veritas\VRTSsfmcs\bin\vomsc.bat` file.
**vxlist**

vxlist - displays records of the Storage Foundation configuration.

**SYNOPSIS**

```
vxlist [-option] [keyword] [arguments] [storage_object_names ...]
```

**DESCRIPTION**

vxlist lists Storage Foundation objects.

To display the vxlist command output, the vxdclid daemon must be running. If vxdclid is not running, run /opt/VRTSsfmh/adm/dclisetup.sh as a root user.

**KEYWORDS**

- alert
  - Lists the alerts.
- cache
  - Lists the Volume Manager cache objects.
- disk
  - Lists the disks.
- diskgroup|dg
  - Lists the Volume Manager disk groups.
- dmp
  - Lists the supported Array Support Libraries (ASL).
- enclosure|enclr|array
  - Lists the enclosures.
- filesystem|fs
  - Lists the mounted file systems.
- hba|hostport|controller|ctrl
  - Lists the controllers.
- lun
  - Lists the Storage Insight Add-on information of LUNs. The information is only available if the host has been added to a Management Server domain, and the associated array has been enabled for Storage Insight.
The first use of the `lun` keyword fetches the array information from Management Server. Any `vxlist lun` command that is run within the next one hour uses the `vxdclid` cache. The `vxdclid` cache may be stale if array parameters have been modified. The `vxlist lun` command that is run after one hour of the last `vxlist lun` command fetches the latest array information from Management Server again.

To force the `vxlist lun` command to fetch the updated array information, use the `rescan` keyword.

`nodeinfo`

Lists the Cluster Volume Manager node information.

`path`

Lists the paths.

`plex|pl`

Lists the plexes.

`rescan`

Fetches updated Storage Foundation information.

See the `lun` keyword.

`snapshot|snap`

Lists the Volume Manager snapshots.

`subdisk|sd`

Lists the subdisks.

`tag|tags`

Lists the volume tags.

`targetport|tca`

Lists the target ports.

`task`

Lists the Volume Manager tasks that are running.

`umfilesystem|umfs`

Lists the unmounted file systems.

`volume|vol`

Lists the Volume Manager volumes.

`vset`

Lists the Volume Manager volume sets.
OPTIONS

- a|--all
   Displays all fields or sections including those that have no data.

- d|--delimiter string
   Uses the specified string instead of spaces to delimit fields in tabular display.

- e|--exact
   Displays all size-related numbers in sectors.
   See the -u option.

- k|--kilobyte
   Displays all size-related numbers in kilobytes.

- g|--diskgroup dg
   Lists storage objects in the specified disk group.

- H|--help [objtype]
   Displays usage information.

- l|--long
   Displays usage information.

- B|--bare field1[,field2...] objtype
   Displays bare format. Displays only the specified long format fields.

- O|--output [csv|long|table]
   Displays information in the selected format. The default is the 'table' format.

- p|--property object_name1 object_name2...
   Displays the property pages of the specified LUNs. The sections without data
   are not displayed unless the --all option is used.

- q|--suppress
   Suppresses headers in tabular output format.

- s|--sections sectionname,... object_name
   Displays only the specified sections in the property page. Sections with no
   data are not displayed unless the --all option is used.

- t|--table [default|lun|stats]
   Displays LUN information in the specified table format. The default format
   is 'default'.

- u|--unit [p|t|g|m|blocks|bytes|scaled]
   Displays all size-related numbers in the specified unit. The default is 'scaled'.
EXAMPLES

This section provides usage examples for `vxlist`.

EXAMPLE 1:  
To display `vxlist` usage for viewing information on disks.
```bash
vxlist -H disk
```

EXAMPLE 2:  
To display the fields Device, Status, Log Info, and VDID for disks, in bare format, delimited by the '++' string.
```bash
vxlist -B "Device,Status,Log Info,VDID" -d ++ disk
```

EXAMPLE 3:  
To display only the disks section in the property page for the volume named `vol_1`.
```bash
vxlist -s disks vol vol_1
```

EXAMPLE 4:  
To display the property pages with the disks section for the volumes named `vol_1` and `vol_2`.
```bash
vxlist -p -s disks vol vol_1 vol_2
```

FILES

/etc/vx/dcli/sfm/conf/dcli_conf.ini
- The `vxlist` and `vxdclid` configuration file

/etc/vx/dcli/log/server_A
- The `vxdclid` log file

NOTES

The default location of `vxlist` is `/opt/VRTSsfmh/bin/vxlist`. There is also a `vxlist` link named `/etc/vx/bin/vxlist`.

Windows-based Management Server does not support the `vxlist` command.
xdistc

xdistc - command-line interface to VRTSsfmh distributor

SYNOPSIS

xdistc [OPTIONS] --push localfile remotefile
xdistc [OPTIONS] --run --command arg1 arg2..
xdistc [OPTIONS] --push localfile remotefile --run --command arg1 arg2..
xdistc --results --id requestid [--wait duration]

DESCRIPTION

xdistc is the command-line interface to the VRTSsfmh distributor. You can use xdistc to copy files or run commands across all managed hosts in a centrally managed domain. You can perform these tasks on the available hosts that are currently running, and on the unavailable hosts when they are started. When you run xdistc, the task that is specified with it continues to run in the background even when xdistc has stopped running.

You can run xdistc only from a Management Server host that has the xprtld daemon running. You must be logged on as root to run xdistc.

OPTIONS

--push localfile remotefile

Copies a file to multiple managed hosts. The symbolic names $TMPDIR, $VARDIR, and $TMPFILE can be used as destination file paths. $TMPDIR typically points to the /tmp directory, but it may vary on Windows managed hosts. $VARDIR points to the /VRTSsfmh/var directory. To use, append the file name after the symbolic name. For example, $TMPDIR/myfile.txt, or $VARDIR/myfile2.txt. $TMPFILE creates a temporary file name ensuring no collision with other files in /tmp. This is useful with the --run option.

You can specify only a few designated directories as the destination. To overwrite existing files while copying, use the --force option.

--run --command arg1 arg2..

Runs a command on multiple managed hosts. In this form, a command is used from commands previously whitelisted on each destination host. The arguments after the double dash are passed directly to the command. You
can specify a request ID with the --id option. If the request ID is not specified, a random ID is internally created.

--push localfile remotefile --run --command arg1 arg2...

Used to copy files and run a command on multiple hosts simultaneously. This option is useful when you want to copy an executable file to multiple managed hosts, and run it.

--results

Retrieves the stdout and stderr results from a run request. You can specify this option with the --run option to view the results of the command that is executed. You must specify the request ID if you use the --results option without the --run option. You can use the --wait option to specify the time the xdistc script should wait to obtain the results.

--os osname

Specifies the operating system. The task that is specified with xdistc is run on the managed hosts that have the specified operating system running. The osname must be specified as one of the following: SunOS, Linux, HP-UX, AIX, Windows. You can also specify multiple operating systems. For example, to specify AIX and Linux, use '/AIX|Linux/', including the single quotes.

--cpu cputype

Specifies the processor. The task that is specified with xdistc is run on the managed hosts that have the specified processor. The cputype must be specified as one of the following: sparc, x86_64, powerpc, x86, x64, i386, i686.

--host hostname

Specifies the host. The task that is specified with xdistc is run on the specified managed host. You can specify the option multiple times to specify multiple hosts.

--hostfile filename

Specifies a file that contains the names of managed hosts. The file must be whitespace delimited. The task that is specified with xdistc is run on the managed hosts that are specified in the file.

--when spec

Specifies the state of the managed hosts. The possible values for spec are 'now', 'up', or 'now,up', without the single quotes. If you specify 'now', the task that you specify with xdistc is run on the managed hosts that are already started. If you specify 'up', the task that you specify with xdistc is run on the managed hosts that are being started or restarted, or the managed hosts...
that are being added to the centrally managed domain. The default value of `spec` is 'now,up'.

`--id requestid`

Specifies the request ID. You can use the `--id` option with the `--push` or `--run` options to assign a request ID. It also collects the output when it is used with the `--results` option. If not specified, an ID is generated internally.

`--ttl timespec`

Specifies the time that `xdistc` should remember the request and the output results of the request. You can specify the time for which `xdistc` should attempt to send the request to the managed hosts. The value of `timespec` can be in days, hours, or minutes. For example, you can use any one of the following values to specify that `xdistc` should remember the request and the output results for a day: `1d`, `24h`, or `1440m`, where `d` stands for days, `h` stands for hours, and `m` stands for minutes. You can also specify one of the following values for `timespec`: 'complete', or 'forever', without the single quotes. If you specify `timespec` as 'complete', `xdistc` deletes the request after it has run the task on the specified hosts. If you specify 'forever', the request is not deleted automatically.

`--wait seconds`

Used with the `--results` option to specify the time the `xdistc` script should wait to obtain the results. You must specify the time in seconds. The default value is 0 seconds, which causes the `xdistc` script to wait indefinitely for the results.

`--force`

Specifies that existing files should be overwritten when files are copied to the managed host.

`--delete`

Specifies that the copied file should be deleted from the managed host after the command that is specified with the `--run` option has completed. The `--delete` option is used only when the `--push` option and the `--run` option are used together.

`--permission p`

Specifies the access permissions for the file that is copied to the managed host. You can specify the access permission as an octal number. For example, 500, or 444.

`--whitename name`

Specifies that after a file is copied, it should be included in the whitelist to be run later.
--user username
   Specifies the user name to be used when the task is run from xdistc on each
   managed host. The default is user name is vxss://sfm_admin//.

--uri uri
   Specifies a raw URI to call. This is a lower-level interface above the --push
   and the --run options that is used to invoke arbitrary URLs.

--d option=value
   Specifies the additional values that xdistc passes as form data to remote
   URLs.

NOTES

The default location of xdistc is /opt/VRTSsfmh/bin/xdistc.
The default log file for xdistc is /var/opt/VRTSsfmh/logs/xdist.log.
Windows-based Management Server does not support the xdistc command.

EXAMPLES

This section provides usage examples for xdistc.

EXAMPLE 1:
To copy the script.sh file to all Linux managed hosts, run it, and display the
results. The file will be deleted from the managed host after it is run. The request
will remain active on Management Server for a day. The command will be sent to
any new hosts joining the domain during this time, and results can be collected
until the request is automatically cleaned up on Management Server.
xdistc --ttl 1d --os Linux --push script.sh /tmp/remote.sh --run
   --delete --results

EXAMPLE 2:
To copy the /root/script.sh file to all managed hosts, set its access permissions,
and whitelist it. The request will remain active on Management Server for a day.
The command will be sent to any new hosts joining the domain during this time,
and results can be collected until the request is automatically cleaned up on
Management Server.
xdistc --ttl 1d --push /root/script.sh /var/opt/VRTSsfmh/script99.sh
   --permission 755 --whitename script99

EXAMPLE 3:
To run the whitelisted `script99` command with arguments. The request will remain active on Management Server for a day. The command will be sent to any new hosts joining the domain during this time, and results can be collected until the request is automatically cleaned up on Management Server.

`xdistc --ttl 1d --run -- script99 arg1 arg2`

**EXAMPLE 4:**

To run `script99` using the whitelist and the lower-level URI interface. The request will remain active on Management Server for a day. The command will be sent to any new hosts joining the domain during this time, and results can be collected until the request is automatically cleaned up on Management Server.

`xdistc --ttl 1d --uri admin/whitelist.pl/run --d argv=["script99","arg1","arg2"]`
Managing Veritas Operations Manager logging

This appendix includes the following topics:

- About log files
- Log file locations

About log files

The Storage Foundation products maintain several log files that operators can use for troubleshooting. You can also configure logging levels that determine what kinds of events are logged.

Log file locations

The following table lists the Veritas Operations Manager log files and their default locations:

---

**Note:** For Veritas Operations Manager on Windows platform, all web application and Web server log files are at `%ALLUSERSPROFILE%\Application Data\Symantec\VRTSfmc\logs\`

For Veritas Operations Manager on UNIX platform, all web application and Web server log files are at `/var/opt/VRTSfmc/logs/`
<table>
<thead>
<tr>
<th>Component</th>
<th>Default location</th>
</tr>
</thead>
</table>
| Veritas Operations Manager service (xprtld) log | Solaris and Red Hat Linux:  
- /var/opt/VRTSsfmh/logs/error.log  
- /var/opt/VRTSsfmh/logs/access.log  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh\logs\error.log  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh\logs\access.log |
| Web applications (Veritas Operations Manager and the other Storage Foundation Web plug-ins) | Solaris and Red Hat Linux:  
- /var/opt/VRTSsfmcs/logs/WebDebugLog.txt.0  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmcs\logs\WebDebugLog.txt.0 |
| Web Server | Solaris and Red Hat Linux:  
- /var/opt/VRTSsfmcs/logs/webserver.log  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmcs\logs\webserver.log |
| Management Server log | Solaris and Red Hat Linux:  
- /var/opt/VRTSsfmh/logs/cs_config.log  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh\logs\cs_config.log |
| Deployment log | Solaris and Red Hat Linux:  
- /var/opt/VRTSsfmh/logs/vxdeploy.log  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh\logs\vxdeploy.log |
<table>
<thead>
<tr>
<th>Component</th>
<th>Default location</th>
</tr>
</thead>
</table>
| Add hosts log | Solaris and Red Hat Linux:  
- /var/opt/VRTSsfmh/logs/add_host.log  
- /var/opt/VRTSsfmh/logs/mhrun.log  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh\logs\add_host.log  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh\logs\mhrun.log  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmcs\logs |
| Management Server log | Solaris and Red Hat Linux:  
- /var/opt/VRTSsfmcs/logs  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmcs\logs |
| Agentlet driver (by family) | Solaris and Red Hat Linux:  
- /var/opt/VRTSsfmh/family/log/mh.log  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmh/family\log\mh.log |
| Database log | Solaris and Red Hat Linux:  
- /varVRTSsfmcs/SFMdb3.log  
Windows:  
- %ALLUSERSPROFILE%\Application Data\Symantec\VRTSsfmcs\db\SFMdb3.log |
Log file locations
Symbols
.csv files 323

A
activities
   viewing 68
activity board message
deleting 68
additional attribute
define 349
   modify 351
   remove 352
additional attributes
   modify value 354
   view 348
alert rule
copying 61
alert rules
deleting 64
   disabling 63
   editing 54
   enabling 62
   modifying 54
   removing 64
alerts
   adding notes 64
   filtering 64
   monitoring 64
analytics gathering on Management Server 28
disable 29
   enable 29
analyzing faults 38
   Faults and Risks 38
application business entity
   creating 194
   editing 203
array ports
display names 151
array ports display name
   setting 151
Arrays
   disabling DMP paths 330
Assign price tier
   processor price tier 240
   server price tier 240
assigning
   price tier 243
Available Patches 153

B
bundling a customized signature
   Distribution Manager Add-on 305
business entities
   change permissions 210
   remove 209
   viewing 201
business entity
   application
      creating 194
      editing 203
   organization
      creating 200
      editing 208
   setting additional attributes 211
   setting extended attributes 211

C
cancel
   deployment log 87
change permissions 210
comma-separated files 323
comparing performance
   disks 168
   file systems 171
   hosts 170
   initiators 169
   volumes 167
Composite business entity 192
Configure
   File system automatic growth 112
configure
  Control Host  119
  Control Host Add-on  119
configure SMTP settings  29
configure VMware discovery 127
configuring web browsers
  Firefox 3.0  21
  Internet Explorer 7.0  21
Control Host  119
  deep array discovery 119
  discover VMware Virtualization
  Infrastructure 119
copying
  alert rule  61
create
  report schedule  316
csv files  323
customized signature
  copying to the managed hosts 304
  creating script  301
  registering on Management Server  304
  using Distribution Manager Add-on  305
customized signatures  300

datastore  125
deep array discovery
  ESX servers  121
default count factor
  UNIX virtual systems  254
  virtual machines  254
  Windows virtual systems  254
defining additional attributes  349
defining extended attributes  349
delete report schedule  319
deleting
  alert rules  64
  policy template  297
deleting activity board message  68
deleting schedules  327
deploying add-ons  73
deploying hotfixes  76
deploying packages or patches  75
deployment log
  cancel  87
  download  88
deployment request details
  view  87
deployment requests
  view  86
deployment summary
  installed OS price tier  260
  number of processors price tier  260
  processor type price tier  260
  server price tier  260
disable report schedule  319
disabling
  alert rules  63
disabling schedules  327
discovering VirtualCenter and ESX servers
  limitations  126
discovering VMware Infrastructure  124
disk performance graphs  163
DMP maintenance case
  Removing a record  344
  Resuming  343
  View results and output  344
DMP Paths
  disabling on an array  330
DMP paths
  Managing  329
  re-enabling  336, 339
download
  deployment log  88
download patch  153
download patch information
  offline mode  156
download schedule
  setting up  155
Dynamic Multipathing  329

edit report schedule  318
editing
  alert rules  54
  VMware discovery configuration  130
enable report schedule  319
enabling
  alert rules  62
  enabling schedules  326
enclosure display name
  setting  149
ESX servers
  datastore  125
  deep array discovery  121
evidence details
  feature  274
Exception
  product inventory deployment issues 234
exceptions
  expired Licenses 234
  High Version Licenses 234
  Multiple Licenses 234
Exceptions tab
  product inventory deployment issues 234
extended attribute
  modify 351
  remove 352
extended attributes
  define 349
  modify value 354
  set values 353
  view 348

F
fault
  fault and dependency view 37
  suppressing 40
  un-suppress 44
  viewing 37
feature
  evidence details 274
feature tracking 274
File system automatic growth
  configuring 112
file system performance graphs 165, 171
File systems
  automatic growth 108
  monitor usage 108
  monitoring 109
filter managed host list 101
Fire drill
  modify fire drill schedule 96
Fire drills
  view schedules 95
Firefox 3.0 21

G
gendeploy.pl 104
Guest LDoms 139

H
high availability objects
  adding to business entity 209
host
  available patches 153
host characteristics
  host make 234
  model 234
  processor count 234
  processor type 234
host performance graphs 162, 170
hosts
  view patches 153

I
ignored violations
  removing 311
initiator performance graphs 164, 169
install
  solution 78
installed signatures
  removing 309
  tunables 308
Internet Explorer 7.0 21

L
LDom discovery 139
  information 142
  limitations 142
  method 141
  prerequisites 140
  requirements 140
LDom Server 139
LDoms
  roles 139
license deployment detailed reports
  exceptions 262
  product details by host name 262
  product details by license key 262
  product evidence 262
  product overview 262
License Deployment Reports
  OS deployment report 234
  product edition deployment report 234
  product name deployment report 234
  product version deployment report 234
License Deployment Summary
  Host deployment summary table 263
License deployment summary table 263
Summary by edition 263
Summary by platform 263
License Deployment Summary (continued)
  Summary by product 263
  Summary by release 263
License Deployment Summary view
  refreshing 234
license deployment views
  scoping 286
License-Host Mapping details
  days remaining until expiration 282
  edition 282
  expiration date 282
  version 282
Licensing and Pricing
  Linux 237
  UNIX
    Per Tiered Processor Meter / Pricing (UxRT 5.x ONLY) 237
    Per Tiered Server Meter / Pricing 237
  Solaris, HP-UX, AIX 237
  Windows 237
list of add-ons 74
log files
  Veritas Operations Manager Web Application 358
Logical Domains discovery 139

M
manage
  reports 313
managed host
  verifying version using the console 24
managed hosts
  adding using gendeploy.pl 104
Management Server
  active users 33
  alert log retention period 31
  configure SMTP settings 29
  download patch 153
  enable analytic gathering 30
  list of active users 28
  managed host details 101
  SMTP details 28
  task log retention period 31
  user session time-out 32
  verifying version using the console 23
  web server log levels 32
  web server session time-out 32
Managing
  DMP paths 329
  managing business entities 190
  security privileges 191
managing hosts from Management Server 100
messages
  viewing 68
Modify
  fire drill schedule 96
modify report schedule 318
modify value
  additional attributes 354
  extended attributes 354
modifying
  alert rules 54
  modifying an additional attribute 351
  modifying an extended attribute 351
Monitor
  file system usage 108
Monitoring
  file system usage 109
O
organization business entity
  creating 200
  editing 208
P
patch details
  viewing 154
performance graphs
  disk 163
  file system 165
  host 162
  initiator 164
  overview 159
  viewing 161–165
  volume 161
policy scan
  scan tunables 310
policy template
  deleting 297
  modifying 296
policy template signature
  removing 309
predefined roles 174
Price tier
  assigning 234
price tier
  assigning 234
price tier (continued)
- uploading 245
- product details by host name 272
- product details by license key edition 279
  - license key serial number 279
  - number of hosts 279
  - platform name 279
  - product name 279
  - version 279
- product evidence 274
- Product Inventory
  - comments 259
  - license deployment heading 259
  - price tier heading 259
- product inventory
  - expired licenses 267
  - invalid licenses 267
  - valid licenses 267
- Product-Tier Mapping summary
  - verification needed 269
- proxy server
  - setting up 155

R
- Re-enabling
  - DMP paths 336, 339
- refresh VirtualCenter server 132
- remove
  - solution 82
- remove report schedule 319
- remove VMware discovery configuration 133
- Removing
  - DMP maintenance record 344
- removing
  - alert rules 64
- removing an additional attribute 352
- removing an extended attribute 352
- removing business entities 209
- removing security groups 188
- report schedule 316
  - disabling 319
  - edit 318
  - enabling 319
- reports
  - archiving 320
  - exporting 323
  - saving
    - archiving reports 320
- reports (continued)
  - saving to file 323
  - virtualization 143
- Resuming
  - DMP maintenance case 343
- roles 174
- rule
  - overview 54

S
- scan tunables
  - viewing 310
- Schedules
  - fire drills 95
- schedules 325
  - deleting 327
  - disabling 327
  - enabling 326
- scope
  - license deployment views 286
- scripts
  - sfmw 358
  - vomsc 359
  - vxlist 361
  - xdistc 365
- security group
  - accessing business entities 210
- security groups
  - removing 188
- set values
  - extended attributes 353
  - object view 353
- set values for extended attributes
  - object view 353
- setting additional attributes
  - business entity 211
- setting extended attributes
  - business entity 211
- setting up download schedule 155
- setting up proxy server 155
- sfmw 358
- signature tunables
  - setting 308
- SMWeb
  - log file 358
  - startup script 358
- solaris zones 134
  - Global Zones 134
  - non-Global Zones 134
solaris zones discovery 134
  information 137
  limitations 138
  method 136
  prerequisites 135
  requirements 135
  utilities 136
solution
  deployment 72
  install 78
  remove 82
  uninstall 81
  upload 77
  view solution deployment summary 82
solutions
  Repository 76
storage enclosures
  display names 149
storage objects
  adding to business entity 209
Summary of Tier-Host Mapping
  Best Match 271
  Exact Match 271
  No Match 271
  User Defined 271
supported add-on versions 74
T
tasks
  viewing 67
Threshold
  File system usage 109
Tier-Host Mapping summary
  price tier legend 261
U
uninstall
  solution 81
upgrade
  managed host 80
upload
  solution 77
  using extended attributes 347
V
verifying
  managed host version using the console 24
  (continued)
    Management Server version using the console 23
Veritas Operations Manager
  performance graphs 159
Veritas Operations Manager Web UI
  starting 25
  stopping 25
view
  deployment request details 87
  solution deployment summary 82
view managed host details 101
viewing
  patch details in SORT Web site 154
  VOM Management Entitlement Report 284
viewing additional attributes 348
viewing extended attributes 348
viewing virtual machines 146
viewing virtualization servers 144
violation
  ignoring 298
virtual machines
  default count factor 254
VirtualCenter server
  refreshing 132
virtualization
  solaris LDom virtualization technology 118
  solaris zones virtualization technology 118
  VMware virtualization technology 118
virtualization management view 126
virtualization reports 143
virtualization summary 143
VMware discovery 121
  configuring 127
  datastore 125
  ESX servers 121
  information 125
  limitations 126
  prerequisites 123
  requirements 123
  VirtualCenter servers 121
VMware discovery configuration
  edit 130
  removing 133
VMware Infrastructure
  discovery 124
  VMware SDK 124
volume performance graphs 161, 167–168
VOM Management Entitlement Report
viewing 284
vomsc 359
vxlist 361

X
xdistc 365

Z
Zone Agentlet 134