

Veritas Storage Foundation™ Manager Dynamic Multipathing Add-on User's Guide

for UNIX

2.0



Storage Foundation Manager Dynamic Multipathing Add-on User'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.

Documentation version 2.0.0

Legal Notice

Copyright © 2008 Symantec Corporation. All rights reserved.

Symantec, the Symantec logo, Veritas, CommandCentral, NetBackup, SANPoint, SANPoint Control, 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 documentation 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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance 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

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance 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 [supportolutions@symantec.com](mailto:supportsolutions@symantec.com)

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support	4	
Chapter 1	About Dynamic Multipathing (DMP) management	9
	About Dynamic Multipathing (DMP) state management	9
Chapter 2	Disabling DMP paths	11
	About the process for identifying active resources	11
	About disabling DMP paths	12
	Starting a new DMP state management case	12
	Start panel options	14
	Select Enclosure panel options	15
	Specify Array Port(s) panel options	16
	Disabling DMP paths	16
	Path Disable Confirmation panel options	17
	DMP State Management Impact Analysis Report	18
	Paths Disabled panel options	19
Chapter 3	Re-enabling DMP paths	21
	About re-enabling DMP paths	21
	Re-enabling DMP paths	22
	Paths Re-Enable Confirmation panel options	23
	Paths Enabled panel options	23
	Advanced DMP Path State Management Result Summary panel options	24
	DMP State Management Waiting Cases view	25
	Resuming an incomplete Centralized DMP State Management case	25
Chapter 4	Managing completed DMP cases	27
	About managing completed DMP state management cases	27
	DMP State Management Completed cases view	27
	Reviewing a completed DMP state management case	28

	Removing a completed Centralized DMP State Management case record	28
	Delete completed case panel	29
Chapter 5	Storage Foundation Manager resources	31
	Storage Foundation Manager on the Web	31
	Getting help	31
	Using the product documentation	32
	Commenting on product documentation	32
	Storage Foundation Manager Glossary	33
	Index	47

About Dynamic Multipathing (DMP) management

This chapter includes the following topics:

- [About Dynamic Multipathing \(DMP\) state management](#)

About Dynamic Multipathing (DMP) state management

Dynamic multipathing (DMP) lets you direct network traffic through different sets of nodes to achieve unlimited failover and load balancing. DMP operates over Fibre Channel, switch-based, and SCSI connections. When a connection fails, DMP spreads network traffic across multiple paths and reroutes traffic automatically.

DMP poses challenges to you when you want to perform maintenance on storage resources. Before you perform maintenance on a storage resource, you must identify the DMP paths that are associated with that storage resource and disable them. After you complete the maintenance on the storage resource, you must re-enable the DMP paths that you disabled.

Before you disable the DMP paths, you must ensure that resources have alternate paths to the underlying physical storage. You must also verify the dependencies of volumes, disk groups, hosts, and applications with the array port associated with the DMP paths.

The DMP State Management Add-on enables you to manage the statuses of the DMP paths that are associated with a storage resource using the Centralized DMP State Management wizard.

As part of DMP state management, you should specify the disc enclosure and the array ports that are associated with the DMP paths that you want to disable. You can specify the disc enclosure and the array ports using the Centralized DMP State Management wizard. Before you proceed with the Centralized DMP State Management wizard, you can also use the Object view to specify the disc enclosure and array ports that are associated with the DMP paths.

After you disable the DMP paths, you can save the DMP state management case and close the wizard. This DMP state management case is saved as a waiting case. After you perform maintenance on the storage resource, you can access this case using the [Total number of DMP cases awaiting user action] case(s) waiting for user action link from the Add-ons view. After you access the case, you can re-enable the DMP paths.

You can save the DMP state management case and close the wizard in the Paths Disabled panel or in the Paths Re-Enable Confirmation panel.

You can view the details of a completed DMP state management case after accessing it using the [Total number of completed DMP cases] case(s) completed link. You can also delete the record of a completed DMP state management case from the DMP state management completed cases view.

See [“DMP State Management Waiting Cases view”](#) on page 25.

See [“DMP State Management Completed cases view”](#) on page 27.

See [“About the process for identifying active resources”](#) on page 11.

See [“Starting a new DMP state management case”](#) on page 12.

See [“Disabling DMP paths”](#) on page 16.

See [“Re-enabling DMP paths”](#) on page 22.

See [“Resuming an incomplete Centralized DMP State Management case”](#) on page 25.

See [“Reviewing a completed DMP state management case”](#) on page 28.

See [“Removing a completed Centralized DMP State Management case record”](#) on page 28.

Disabling DMP paths

This chapter includes the following topics:

- [About the process for identifying active resources](#)
- [About disabling DMP paths](#)
- [Starting a new DMP state management case](#)
- [Disabling DMP paths](#)

About the process for identifying active resources

In a typical scenario, the operator begins by setting a scope for the operation. In the example of an array port, this involves specifying the name of the port for which maintenance will be performed.

After identifying a port for maintenance, the operator can view a list of other resources (disks, volumes, and applications) that have dependencies on the port, along with information about the paths over which they connect to the port.

The Impact Analysis Report helps you understand the relationship between the disabled DMP paths and the storage resources that are associated with them

Similarly, other network maintenance—for example, a firmware upgrade or an HBA upgrade—requires that the resource not be part of a currently active DMP path. Maintenance and upgrades can be performed only for nodes that are not on an active path.

Although it is easy to verify whether a single resource, or node, is on an active path, it is much harder when, as is often the case, an administrator wants to perform the upgrade on several nodes simultaneously.

The same verification must be done for other situations as well, such as data migration. Internal audits can also require you to verify path status for several

network resources simultaneously—verifying, for example, that critical data is protected by multiple paths.

In all of these maintenance scenarios, the SF Manager provides an easy way to identify the current active DMP path on multiple nodes simultaneously.

Any resource that does not have additional paths to its underlying storage is highlighted in the display, because such a resource would be completely unavailable when maintenance is performed on the array port.

About disabling DMP paths

After you identify the DMP paths that are associated with the storage resource that you want to maintain, you must disable the DMP paths. Use the DMP state management wizard to disable the DMP paths. You can launch this wizard from either the Add-ons view or the Object view.

See [“About the process for identifying active resources”](#) on page 11.

See [“Starting a new DMP state management case”](#) on page 12.

See [“Disabling DMP paths”](#) on page 16.

Starting a new DMP state management case

You can start a new Centralized DMP State Management case to disable the DMP paths that are associated with a storage resource.

You can start a new Centralized DMP State Management case either from the Add-on view or from the Object view.

In the Add-on view, click the Start new Centralized State Management case link to launch the DMP state management wizard.

In the Object view, you can specify the disk enclosure and the array port that are associated with the DMP paths that you want to disable.

If you specify the array port in the Object view, the Select Enclosure panel is not displayed when you proceed with the DMP state management case. In this case, after specifying the name for the Centralized DMP State Management case, you are directed to the Specify Array Port(s) panel. The array ports that you have selected in the Object view appear checked in the Specify Array Port(s) panel. You can modify the selection of array ports on this panel.

To start a new Centralized DMP State Management case from the Add-ons view

- 1 In the Add-ons view, click the **Start new Centralized State Management case** link.
- 2 In the Start wizard panel, enter the details and click **Next**.
See “[Start panel options](#)” on page 14.
- 3 In the Select Enclosure panel, select the disk enclosure that contains the array ports on which you want to disable the associated DMP paths and click **Next**.
See “[Select Enclosure panel options](#)” on page 15.
- 4 In the Specify Array Port(s) panel, select one or more array ports on which you want to disable the associated DMP paths and click **Next**.

Note: When you select an array port, all the DMP paths that are associated with that array port are also selected.

See “[Specify Array Port\(s\) panel options](#)” on page 16.

To start a new Centralized DMP State Management case from Objects view

- 1 Select **Managing > Storage > Enclosure**.
- 2 In the enclosure view, do one of the following:
 - Check the disk enclosure that contains the array ports on which you want to disable the associated DMP paths. From the task drop-down list, select the **DMP State Management** option and click **GO**.
 - Click the name of the enclosure that you have selected to get the Enclosure Overview view. In the left panel under **Add-ons**, click **DMP State Management**.
 - Click the name of the enclosure that you have selected to get the Enclosure Overview view. Click the Array Ports tab. Select one or more array ports on which you want to disable the associated DMP paths. From the task drop-down list, select the **DMP State Management** option. Click **GO**.

- Click the name of the array port that you have selected to get the Array Ports Overview view. In the left panel under **Add-ons**, click **DMP State Management**.
- 3 In the Start wizard panel, enter the details and click **Next**.
See “[Start panel options](#)” on page 14.

Note: The Select Enclosure panel is not displayed because you have already selected the array ports on which you want to disable the associated DMP paths. If you specify one or more array ports on which you want to disable the associated DMP paths, the Select Array Port(s) panel displays those array ports only.

- See “[Specify Array Port\(s\) panel options](#)” on page 16.
See “[About Dynamic Multipathing \(DMP\) state management](#)” on page 9.
See “[About disabling DMP paths](#)” on page 12.
See “[Disabling DMP paths](#)” on page 16.

Start panel options

Use this wizard panel to start a new DMP state management case or resume a DMP state management case.

This panel lets you specify a name for a new Centralized DMP State Management case that you want to start. You can refer to the Centralized DMP State Management case with this name.

To resume an incomplete Centralized DMP State Management case, select the case name from this panel.

Table 2-1 Start panel options

Field	Description
Start New DMP State Management Case	Begins a new Centralized DMP State Management case.
Case Name	Name of the new Centralized DMP State management case that you want to start. You can reference the Centralized DMP State Management case with the name that you have specified on this field.

Table 2-1 Start panel options (*continued*)

Field	Description
Description	Additional information that you want to include for the new Centralized DMP State Management case. This field is optional.
Resume Existing DMP State Management Case	Resumes an incomplete Centralized DMP State Management case that you want to complete.
Unfinished Cases	Select the incomplete Centralized DMP State Management case that you want to complete.

See [“Starting a new DMP state management case”](#) on page 12.

Select Enclosure panel options

Use this wizard panel to select the disk enclosure that contains the array ports on which you want to disable the associated DMP paths.

This panel lists the disk enclosures available in the database and uses DMP on exported LUNs. It does not list the disk enclosures that do not use DMP.

Select the enclosure that contains the array ports on which you want to disable the DMP paths. When you select the option, the row that represents the enclosure is highlighted.

Table 2-2 Select Enclosure panel options

Field	Descriptions
Name	Name of the disk enclosure that you have selected
Serial	Serial number of the disk enclosure that you have selected
Vendor	Name of the vendor who supplied the disk enclosure that you have selected
Product	Name of the array model
Type	Type of array
(Total)	Total number of disk enclosures that are listed in the panel

See [“Starting a new DMP state management case”](#) on page 12.

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 following in a tree structure:

- All the array ports within a selected disk enclosure
- Hosts that are connected to the array port
- Disk group that is associated with the array port
- Paths associated with the array port

Select one or more array ports on which you want to disable the associated DMP paths.

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 single path that is associated with an array port. Single paths are highlighted in red.

See [“Starting a new DMP state management case”](#) on page 12.

Disabling DMP paths

Use the Path Disable Confirmation panel and the Path Disabled panel on the DMP state management case wizard to disable the DMP paths.

You can launch an Impact Analysis Report from this panel. The Impact analysis Report helps you understand the relationship between the disabled DMP paths and the storage resources that are associated with them.

To disable the DMP paths

- 1 In the Path Disable Confirmation panel, view the details of the DMP paths that you have selected for disabling and click **Next**.
See [“Path Disable Confirmation panel options”](#) on page 17.
- 2 Click the **View Impact Analysis Report** link to view the applications and dependencies on the DMP paths that are displayed on this wizard.
See [“DMP State Management Impact Analysis Report”](#) on page 18.
- 3 In the Paths Disabled panel, view the output summary of the DMP path disable operation and click **Save&Close**.

Note: The panel is closed after saving the DMP State Management case. The DMP paths that you have selected are disabled. Now, you can perform maintenance on the storage resource.

See [“Paths Disabled panel options”](#) on page 19.

See [“About Dynamic Multipathing \(DMP\) state management”](#) on page 9.

See [“About disabling DMP paths”](#) on page 12.

See [“About the process for identifying active resources”](#) on page 11.

See [“Starting a new DMP state management case”](#) on page 12.

See [“Re-enabling DMP paths”](#) on page 22.

See [“Resuming an incomplete Centralized DMP State Management case”](#) on page 25.

Path Disable Confirmation panel options

Use this wizard panel to view the details of the DMP paths that you have selected for disabling.

On this panel, you can see the following:

- Name of the Centralized DMP State Management case
- Details of the disk enclosure that contains the array ports on which you want to disable the associated DMP paths

This wizard panel also lists the following details:

- DMP paths that you have selected for disabling
- Array port to which these paths are associated
- Host to which these paths are connected

- HBA associated with the host to which these paths are connected
- Current status of these paths
- Disk Group association
- Disk association

You can click the Impact Analysis Report link to view the relationship between the DMP paths that you want to disable and the storage resources that are associated with them.

Table 2-3 Path Disable Confirmation panel options

Field	Description
Name	Names of the DMP paths that you have selected for disabling
Array Port	Array Port to which the DMP Paths that you have selected for disabling is associated
Host	Host to which the DMP Paths that you have selected for disabling is connected
HBA	HBA associated with the host to which the DMP Paths that you have selected for disabling is connected
Status	Current status of the DMP Paths that you have selected for disabling
(Total)	Total number of DMP Paths that you have selected for disabling

See [“Disabling DMP paths”](#) on page 16.

DMP State Management Impact Analysis Report

Use this wizard panel to understand the relationship between the disabled DMP paths and the storage resources that are associated with them. This report helps you identify any probability for path failure. You can take precautions to avert such failures and ensure the availability of the storage resource online.

Table 2-4 DMP State Management Impact Analysis Report fields

Field	Description
Selected Enclosure	Name of the enclosure that contains the array ports to which the disabled DMP paths are associated
Case Name	Name of the DMP state management case that you currently process
Dependencies for Array Port	Array port on which you want to disable the associated DMP paths

See [“Disabling DMP paths”](#) on page 16.

See [“About the process for identifying active resources”](#) on page 11.

Paths Disabled panel options

Use this wizard panel to view the output summary of the DMP path disabling operation.

This panel displays the name of the DMP State Management case that you are currently processing. It also displays the name of the enclosure that contains the array ports with which the disabled DMP paths are associated.

Table 2-5 Path Disabled panel options

Field	Description
Path Disable Operation Output Summary	<ul style="list-style-type: none"> ■ Total number of commands that successfully disabled the DMP paths ■ Total number of commands that failed to disable the DMP paths, if any.
Command Details	<ul style="list-style-type: none"> ■ Hosts on which the commands that successfully disabled the DMP paths are executed ■ Details of the DMP paths that are disabled ■ Details of the commands that failed to disable the DMP paths, if any, and the reason for the failure.

See [“Disabling DMP paths”](#) on page 16.

Re-enabling DMP paths

This chapter includes the following topics:

- [About re-enabling DMP paths](#)
- [Re-enabling DMP paths](#)
- [DMP State Management Waiting Cases view](#)
- [Resuming an incomplete Centralized DMP State Management case](#)

About re-enabling DMP paths

After you finish maintenance on a storage resource, you must re-enable the associated DMP paths.

To re-enable the DMP paths, continue with the Paths Re-Enable Confirmation and the Paths Enabled panels on the Centralized DMP State Management case wizard.

If you close the Centralized DMP State Management wizard after disabling the DMP paths, you must relaunch the DMP state management case wizard to re-enable them. You can relaunch the wizard from the DMP State Management Waiting Cases view.

See [“Re-enabling DMP paths”](#) on page 22.

See [“DMP State Management Waiting Cases view”](#) on page 25.

See [“Resuming an incomplete Centralized DMP State Management case”](#) on page 25.

Re-enabling DMP paths

Use the Paths Re-Enable Confirmation and the Paths Enabled panels in the DMP State Management wizard to re-enable the DMP paths. You disable these paths before you perform maintenance on the storage resource.

The Paths Re-enable Confirmation panel displays the details of the DMP paths that you want to re-enable.

The Path Enabled panel displays the output summary of the DMP paths re-enable operation. On this panel, you can view the path re-enable commands that succeed and the path re-enable commands that fail.

To re-enable the DMP paths

- 1 After you perform maintenance on the storage resource, launch the Paths Disabled panel again and click **Next**.
 - 2 In the Paths Re-Enable Confirmation panel, view the details of the DMP paths that you want to re-enable and do one of the following:
 - To save the DMP state management case and close the panel, click **Save & Close**.
 - To re-enable the DMP paths, click **Next**.
See [“Paths Re-Enable Confirmation panel options”](#) on page 23.
 - 3 In the Paths Enabled panel, view the output summary of the path re-enable operation and click **Next**.
See [“Paths Enabled panel options”](#) on page 23.
 - 4 In the Advanced DMP Paths State Management Result Summary panel, view the details of the DMP paths that you have managed and click **Close**.
See [“Advanced DMP Path State Management Result Summary panel options”](#) on page 24.
- See [“About Dynamic Multipathing \(DMP\) state management”](#) on page 9.
- See [“DMP State Management Waiting Cases view”](#) on page 25.
- See [“About re-enabling DMP paths”](#) on page 21.
- See [“Disabling DMP paths”](#) on page 16.
- See [“Resuming an incomplete Centralized DMP State Management case”](#) on page 25.

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.

This panel displays the name of the Centralized DMP State Management case that you are processing. It also displays the details of the disk enclosure that contains the array ports on which you want to re-enable the associated DMP paths.

Table 3-1 Paths Re-enable Confirmation panel options

Field	Description
Name	Name of the DMP paths that you want to re-enable
Array Port	Array port to which the DMP Paths that you want to re-enable is associated
Host	Host to which the DMP Paths that you want to re-enable is connected
HBA	HBA associated with the host to which the DMP Paths that you want to re-enable is connected
(Total)	Total number of DMP Paths that you want to re-enable

See [“Re-enabling DMP paths”](#) on page 22.

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 Centralized DMP State Management 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 the commands that successfully executed. You can also view the path enable commands that failed.

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 DMP paths”](#) on page 22.

Advanced DMP Path State Management Result Summary panel options

Use this wizard panel to view the overall summary of the DMP path state management that you have completed.

This panel lists the following details:

- DMP paths that you have managed and their current statuses
- All commands that are executed during the DMP path state management operation and their results

Table 3-2 Advanced DMP Path State Management Result Summary panel options

Field	Description
Name	Name of the DMP path on which you have completed the state management
Array Port	Array port with which the DMP paths on which you have completed the state management is associated
Host	Host with which the DMP path on which you have completed the state management is connected
HBA	HBA associated with the host
Status	Current status of the DMP path on which you have completed the state management
(Total)	Total number of DMP paths on which you have completed the state management

Under All Commands Executed and Results, you can view the following details:

- The commands that failed to disable the DMP paths, if any
- The commands that disabled the DMP paths
- The commands that failed to re-enable the DMP paths, if any
- The commands that re-enabled the DMP paths

See [“Re-enabling DMP paths”](#) on page 22.

DMP State Management Waiting Cases view

This view lists the incomplete DMP cases that you have saved after disabling the DMP paths. You can select these incomplete DMP cases to re-enable the DMP paths that you have disabled. You disable the paths before you perform maintenance on the storage resource.

To access this view, in the Add-ons view, click the [Total number of waiting cases] case(s) waiting for user action link.

See [“About Dynamic Multipathing \(DMP\) state management”](#) on page 9.

See [“DMP State Management Completed cases view”](#) on page 27.

See [“About re-enabling DMP paths”](#) on page 21.

See [“Resuming an incomplete Centralized DMP State Management case”](#) on page 25.

Resuming an incomplete Centralized DMP State Management case

In the DMP State Management Waiting Cases view, select the Resume case and Re-enable path option to resume the DMP case.

To resume an incomplete DMP state management case

- 1 In the Add-ons view, click the **[Total number of waiting cases] case(s) waiting for user action** link.
- 2 In the DMP State Management Waiting Cases view, under Waiting Cases, check the incomplete DMP case name that you want to resume.
- 3 From the tasks drop-down list, select the **Resume case and Re-enable Paths** option and click **GO**.

See [“Disabling DMP paths”](#) on page 16.

See [“Re-enabling DMP paths”](#) on page 22.

See [“About Dynamic Multipathing \(DMP\) state management”](#) on page 9.

Managing completed DMP cases

This chapter includes the following topics:

- [About managing completed DMP state management cases](#)
- [DMP State Management Completed cases view](#)
- [Reviewing a completed DMP state management case](#)
- [Removing a completed Centralized DMP State Management case record](#)

About managing completed DMP state management cases

After you perform maintenance on a storage resource and re-enable the DMP paths that are associated with it, you can review the output of a completed Centralized DMP State Management case. You can also remove the record of a completed DMP state management case.

See [“DMP State Management Completed cases view”](#) on page 27.

See [“Reviewing a completed DMP state management case”](#) on page 28.

See [“Removing a completed Centralized DMP State Management case record”](#) on page 28.

DMP State Management Completed cases view

In this view, you can review the output of a completed DMP state management case or remove the record of a completed DMP state management case.

To access this view, on the Add-ons view, click the [Total number of completed DMP cases] completed link.

See [“About Dynamic Multipathing \(DMP\) state management”](#) on page 9.

See [“DMP State Management Waiting Cases view”](#) on page 25.

See [“About managing completed DMP state management cases”](#) on page 27.

See [“Reviewing a completed DMP state management case”](#) on page 28.

See [“Removing a completed Centralized DMP State Management case record”](#) on page 28.

Reviewing a completed DMP state management case

In the DMP State Management Completed cases view, you can select the Show Case Output and Results option to view the details of the completed Centralized DMP State Management case output.

To review a completed DMP State management case

- 1 In the Add-ons view, click the **[Total number of DMP case(s) that are completed] case(s) completed** link.
- 2 In the DMP State Management Completed Cases view, under Completed Cases, view the details of the completed DMP state management cases.
- 3 Check the DMP case name that you want to review.
- 4 From the task drop-down list, select the **Show Case Output and Results** option and click **GO**.

See [“Removing a completed Centralized DMP State Management case record”](#) on page 28.

See [“About Dynamic Multipathing \(DMP\) state management”](#) on page 9.

Removing a completed Centralized DMP State Management case record

In the DMP State Management Completed cases view, select the Delete Cases option to remove the record of a completed DMP state management case.

To remove a completed Centralized DMP State Management case

- 1 In the Add-ons view, click the **[Total number of DMP case(s) that are completed] case(s) completed** link.
- 2 In the DMP State Management Completed Cases view, under Completed Cases, view the completed Centralized DMP State Management cases.
- 3 Check the DMP case name that you want to remove.
- 4 From the task drop-down list, select the **Delete Cases** option and click **GO**.
- 5 In the Delete Complete Case panel, click **Yes**.

See [“Delete completed case panel”](#) on page 29.

See [“Reviewing a completed DMP state management case”](#) on page 28.

See [“About Dynamic Multipathing \(DMP\) state management”](#) on page 9.

Delete completed case panel

Use this panel to confirm the removal of a completed Centralized DMP State Management case record.

See [“Removing a completed Centralized DMP State Management case record”](#) on page 28.

Removing a completed Centralized DMP State Management case record

Storage Foundation Manager resources

This chapter includes the following topics:

- [Storage Foundation Manager on the Web](#)
- [Getting help](#)
- [Using the product documentation](#)

Storage Foundation Manager on the Web

For comprehensive, up-to-date information about SF Manager, visit the Symantec Web site:

www.symantec.com/sfm

Getting help

If an issue arises while you use the products, refer to the product documentation and online help. If necessary, report it to Symantec.

For technical assistance, visit

www.symantec.com/enterprise/support/index.jsp

This site provides access to resources such as TechNotes, product alerts, software downloads, hardware and software compatibility lists, and the customer email notification service. Use the Knowledge Base Search feature to access additional product information, including current and past releases of product documentation.

Using the product documentation

The following guides provide information about Storage Foundation Manager:

- *Veritas Storage Foundation Manager Administrator's Guide*
- *Veritas Storage Foundation Manager Getting Started Guide*
- *Veritas Storage Foundation Manager Installation Guide*

For complete host operating system and system resource specifications, as well as any known limitations or issues in this release, see the *Veritas Storage Foundation Manager Release Notes*.

Commenting on product documentation

Submit comments about the product documentation to the following email address:

storage_management_docs@symantec.com

Please include the following information with your documentation comments:

- The title and product version of the guide you are commenting on
- The topic (if relevant) you are commenting on
- Your comment
- Your name

Glossary

Action Agent	A component, residing on the Management Server, that provides end users with the ability to create rules triggered by alerts from the Veritas Provider Access Layer (VxPAL). These rules, or policies, associate certain sets of conditions with storage resources and define actions to be taken when these conditions are detected. The Action Agent is seamlessly integrated with the SF Manager so that users of the Console can monitor, define, and modify policies. Also Rule Manager.
Active/active configuration	A failover configuration where each system runs a service group. If either system fails, the other one takes over and runs both service groups. Also symmetric configuration.
Active/passive configuration	A failover configuration consisting of one service group on a primary system, and one dedicated backup system. Also asymmetric configuration.
addressable storage	Configured storage that has been apportioned into addressable units (LUNs) and is ready to be allocated to hosts. This storage is typically part of RAID groups.
addressable unit	Any storage resource in the network that is ready to be allocated for use by hosts and applications. Also AddrUnit or AU. See also LUN
agent	A process running on a managed host that collects status information from network resources, such as hardware and virtual storage, and relays that information to the Management Server. See also explorer In VCS, a process that starts, stops, and monitors all configured resources of a type, and reports their status to VCS.
Agent	See managed host
Alarm Service	A component (Windows service/UNIX daemon), residing on the Management Server, that retrieves and correlates SNMP and other data and sends alerts to the Action Agent for further processing using defined policies. The Alarm Service has a command-line interface— <code>vxascmd</code> —with which you can connect to the Alarm Service to obtain server and object information and perform various Alarm Service commands and queries.
alert	One of several types of configurable notifications produced when an Action Agent alarm is triggered. An alert is dynamic, resetting itself automatically when a condition monitored by a policy returns to its specified CLEAR state.

Alert Manager	See Action Agent
allocated storage	<p>The total amount of addressable storage in LUNs that is designated for use by specific hosts. A LUN is considered allocated when a host operating system has written a device handle for the LUN (in other words, claimed the LUN) or when the array has masked the LUN to a specific target.</p> <p>Contrast with unallocated storage</p>
annotation	<p>A user-defined tag (attribute) that can be applied to a resource or set of resources. It represents information that cannot be discovered by SF Manager. Each annotation consists of an attribute, for example LOCATION, and can be given one or more values, for example 2ND FLOOR. Annotations are useful for organizing resources according to their shared characteristics. They are also used for assigning storage to tiers. SF Manager supports two kinds of annotations: host-specific annotations, which are defined on a host through a standalone product such as VxVM or VVR; and global annotations, which are stored only in the SF Manager database.</p>
application	<p>A program or group of programs designed to perform a specific task. Oracle Database and Symantec NetBackup are examples of applications.</p>
big-endian	<p>A technique for multibyte data storage in which the most significant value in each sequence is stored at the lowest (that is, first) storage address.</p> <p>Contrast with little-endian</p>
bridge	<p>A device that connects and passes packets between two segments of a storage network that use the same communications protocol.</p> <p>See also router</p>
capacity	<p>The amount of storage an object can allocate or use.</p>
centralized mode	<p>The condition in which a constituent product or plug-in product [point product] is running on the Management Server, in conjunction with other constituent products. This is the opposite of the situation in which the product runs by itself.</p>
claimed storage	<p>Storage for which at least one host's operating system has created a device handle.</p> <p>Contrast with unclaimed storage</p>
cluster	<p>A set of hosts (each termed a node) that share a set of disks and are connected by a set of redundant heartbeat networks. A cluster can have from one to 32 member systems, or nodes. Also VCS cluster.</p>
cluster communication	<p>Communication between clusters using either of the two core communication protocols defined by Symantec Cluster Server: GAB and LLT. The communication takes place by means of heartbeat signals sent between systems or fast kernel-to-kernel broadcasts.</p>
Cluster Server	See Veritas Cluster Server (VCS)

collector	A measurement representing a specific state or numerical value for objects in the storage network. The Alarm Service uses collectors to monitor and correlate status and performance information, using several different processes. The Alert Manager uses information gathered by collectors to trigger actions such as SMTP mail, Console alerts, commands, and logging.
CommandCentral Storage	A product offering designed to maximize the return on an enterprise's storage technology investment by providing tools with which a storage administrator can make the storage network or SAN operate as effectively as possible.
configured storage	Physical storage that has been formatted and is ready to be apportioned into RAID groups. Contrast with unconfigured storage
connectivity plan	A customizable report with which an operator can see the dependencies between the logical storage resources provided by Veritas Volume Manager and the underlying physical storage, and verify the connections to that storage as visible from various hosts on the network.
deport	To disable all local access to a VxVM-managed disk group or volume, usually in preparation for moving it. Contrast with import
device	A collective term for disks, tapes, disk arrays, tape arrays, and any other objects that store data. Also storage device.
device handle	The name the operating system uses to identify a storage resource (known as an addressable unit or LUN), and the correct means (driver, system call) to access it. Also OS handle.
disaster recovery	The use of a secondary location to recover applications and data after a site failure. Disaster recovery requires heartbeating and replication.
discovery	The process of finding objects on the storage network and adding information about them to a database. See also explorer
disk group	A collection of disks that share a common configuration. A disk group configuration is a set of records containing detailed information on existing Veritas Volume Manager objects (such as disk and volume attributes) and their relationships. Each disk group has an administrator-assigned name and an internally defined unique ID. The root disk group (rootdg) is a special private disk group that always exists.
Domain Controller	A server component that provides an infrastructure and communications layer for object and cache management for many Symantec storage management products. In SF Manager the Domain Controller is installed on the Management Server. Also <code>vxsvc</code> .

Contrast with Local Controller

Dynamic Multipathing (DMP)	A feature of Veritas Volume Manager designed to provide greater reliability and performance by using path failover and load balancing for multiported disk arrays connected to host systems through multiple paths. DMP detects the various paths to a disk using a mechanism that is specific to each supported array type. DMP can also differentiate between different enclosures of a supported array type that are connected to the same host system.
Dynamic Storage Tiering (DST)	A feature with which administrators of multi-volume VxFS file systems can manage the placement of files on individual volumes in a volume set by defining placement policies that control both initial file location and the circumstances under which existing files are relocated. These placement policies cause the files to which they apply to be created and extended on specific subsets of a file system's volume set, known as placement classes. The files are relocated to volumes in other placement classes when they meet specified naming, timing, access rate, and storage capacity-related conditions. See also Veritas File System (VxFS)
event	A notification that indicates when an action, such as an alert or a change in state, has occurred for one or more objects on the storage network.
explorer	A software tool that uses a unique methodology to discover information about a particular kind of resource on the storage network. In an SF Manager configuration, explorers running on both the Management Server and the managed host locate resources and discover information about them. See also discovery
extent	A continuous space on a disk or storage volume that is occupied by or reserved for a particular data set, data space, or file.
fabric	A group of SAN objects connected by a Fibre Channel (FC) switch. A fabric contains at least one FC switch and may also contain zones.
failover	A backup operation that automatically switches to a standby database, server, or network if the primary system fails or is temporarily shut down for servicing.
Fibre Channel	A collective name for the fibre optic technology that is commonly used to set up a storage area network (SAN) or virtual fabric (VSAN). A set of standards capable of transferring data between ports and through network devices at higher speeds and over significantly greater distances than SCSI technology, Fibre Channel supports point-to-point, loop, and fabric topologies.
file change log (FCL)	In Veritas File System, a repository to track changes made to files in a file system. It can also contain information about file accesses (such as opens, reads, and writes) and I/O activity. FCL data is used in file placement policies to evaluate a file's activity level (access history and I/O temperature).

file system	A means of organizing the addressable storage of one or more physical or virtual disks to give users and applications a convenient way of organizing files. File systems appear to users and applications as directories arranged in a hierarchy.
firmware	A set of software instructions set permanently in a device's memory.
GBIC	Gigabit interface converter. A widely used transceiver module for Fibre Channel. A GBIC is modular and hot-swappable and can be either copper or optical.
generic group	<p>A class or collection of switches, hosts, and storage devices. Groups are useful for a number of different purposes such as meeting certain availability and redundancy requirements, or for administrative or tracking purposes.</p> <p>See also group</p>
Global Service Group	A VCS service group that spans across two or more clusters. The ClusterList attribute for this group contains the list of clusters over which the group spans.
group	A class or collection of network objects. Groups are useful for a number of different purposes such as meeting certain availability and redundancy requirements, or for administrative or tracking purposes. The SF Manager supports two different types of groups: custom groups (user-defined collections of objects) and application groups (collections of objects determined by their common dependency on a specific application).
Group Atomic Broadcast (GAB)	A communication mechanism of the VCS engine that manages cluster membership, monitors heartbeat communication, and distributes information throughout the cluster.
HBA	Host bus adapter. An interface between a server or workstation bus and a Fibre Channel network.
heartbeat	A signal sent at regular intervals to indicate that a host and its connections are operating normally.
High Availability (HA)	The concept of configuring the SF Manager to be highly available against system failure on a clustered network using Symantec Cluster Server (VCS).
hub	A common connection point for devices in the storage network. The hub may be unmanaged, IP-managed, or FC-managed. An unmanaged hub is passive in the sense that it serves simply as a conduit for data, moving the data from one storage resource to another. IP-managed and FC-managed hubs are intelligent, containing features an administrator can use to monitor the traffic passing through the hub and configure each port in the hub.
import	<p>To re-enable local access to a VxVM-managed disk group or volume, usually after it has been moved.</p> <p>Contrast with deport</p>

in-band	<p>A type of Fibre Channel management protocol. The most prevalent in-band protocol over Fibre Channel is SCSI Enclosure Services (SES).</p> <p>Contrast with out-of-band</p>
intent	<p>A conceptualization of the purpose of a disk or a volume. Connectivity reports in the SF Manager Console display data on intent satisfaction: a measure of how closely the storage device's actual usage aligns with its intended purpose.</p>
IP address	<p>An identifier for a computer or other device on a TCP/IP network, written as four eight-bit numbers separated by periods. Messages and other data are routed on the network according to their destination IP addresses.</p> <p>See also virtual IP address</p>
jeopardy	<p>The state in which a node is missing one of the two required heartbeat connections. When a node is running with one heartbeat only (in jeopardy), VCS does not restart the applications on a new node. This action of disabling failover is a safety mechanism that prevents data corruption.</p>
legacy managed host	<p>A Storage Foundation version 4.x host that contains a Veritas Provider Access Layer (VxPAL) agent enabling it to be centrally managed by Storage Foundation Manager.</p>
little-endian	<p>A technique for multibyte data storage in which the most significant value in each sequence is stored at the highest (that is, last) storage address. Contrast with big-endian</p>
Local Controller	<p>A server component that provides object and cache management for many Symantec storage management products. In SF Manager the Local Controller can be installed on a Management Server or on a standalone host, where it also functions as a daemon for the Veritas Enterprise Administrator (Enterprise Administrator) Java console to connect to and manage the host. Also <code>vxsvc</code>.</p> <p>Contrast with Domain Controller</p>
logical volume	<p>A simple volume that resides on an extended partition on a basic disk and is limited to the space within the extended partitions. A logical volume can be formatted and assigned a drive letter, and it can be subdivided into logical drives.</p> <p>See also LUN</p>
LUN	<p>Acronym for "logical unit number." A unique and discrete addressable unit or logical volume that may reside inside one or more simple or array storage devices. LUNs are exposed to the outside world through an addressing scheme presented to the host as SCSI LUN numbers. Each LUN has a unique device handle and represents a logical volume.</p>
LUN binding	<p>The creation of access paths between an addressable unit (AddrUnit) within a disk array and a port on the array. AddrUnits are storage volumes built out of the physical disks within the array. Array ports are connected to the SAN fabric and</p>

function as SCSI targets behind which the AddrUnits bound to those ports are visible.

LUN masking	The practice of enabling access to a particular addressable unit (AddrUnit) for a host on the storage network. This is done by creating an access control list associated with the LUN (the access path) between that AddrUnit and an array port to which it is bound. The access control list for a LUN contains the World Wide Name of each HBA port that is allowed to access that LUN within the array.
managed host	<p>A component that assists the Management Server in discovering all of the resources in the storage network. The managed host is connected to the Management Server and consists of several agents that are also used by the Management Server.</p> <p>See also agent</p>
management explorer (MGEX)	An explorer that uses the Fibre Channel Common Transport (CT) protocol to discover switches in-band over Fibre Channel, obtain switch characteristics, and explore port connectivity.
Management Server	The central component in a Storage Foundation Manager installation. It receives network data from one or more managed hosts and serves as a focal point for various network management operations.
mirroring	A form of storage redundancy in which two or more identical copies of data are maintained on separate volumes. (Each duplicate copy is known as a mirror.) Also RAID Level 1.
multipathing	<p>Multiple physical access paths to a disk connected to a host system. Any software residing on the host (for example, the DMP driver) that hides multiple physical access paths from the user is said to provide multipathing functionality.</p> <p>See also Dynamic Multipathing (DMP)</p>
network partition	<p>The condition that exists after all network connections between any two groups of systems fail simultaneously. When this happens, systems on both sides of the partition can restart applications from the other side resulting in duplicate services, or split-brain. A split brain occurs when two independent systems configured in a cluster assume they have exclusive access to a given resource (usually a file system or volume). The most serious problem caused by a network partition is that it affects the data on shared disks.</p> <p>See jeopardy</p> <p>See seeding</p>
node	<p>An object in a network. In Symantec Cluster Server, node refers specifically to one of any number of hosts in a cluster.</p> <p>See also object</p>

object	A single, unique addressable entity on a storage network. It is possible for objects to be present within objects. For example, while a tape array is an object, each individual tape drive within the array is also an object. A host is an object, and the HBA inside the host is also an object. Each object has one or more attributes and can be a member of one or more zones.
object dependency group	A class or collection of storage objects associated with applications, such as volumes and file systems. Groups are useful for a number of different purposes such as meeting certain availability and redundancy requirements, or for administrative or tracking purposes. See also group
Object Reference or OID (Object ID)	A key which uniquely identifies an object in the discovery data store. OIDs are represented in XML files as hexadecimal strings with a maximum length of 128 characters.
out-of-band	A type of communication protocol other than the Fibre Channel management protocol, such as SNMP or a vendor-specific proprietary protocol. Contrast with in-band
path	The route through which a host accesses data on a storage medium such as a disk in an array. The path consists of an HBA (host bus adapter) on the host, a SCSI or Fibre Channel connector, and a controller on the disk or disk array.
physical fabric	The physical components of a fabric, including all switches and all other SAN objects. You can configure one or more virtual fabrics—each one isolated from the others—based on the hardware components in the physical fabric.
plex	In storage media managed by Veritas Volume Manager (VxVM), a collection of one or more subdisks located on one or more physical disks. See also subdisk volume
policy	A set of rules, or configuration settings, that are applied across a number of objects in the storage network. You establish policies to help you monitor and manage the network. Each policy associates certain sets of conditions with storage resources and defines actions to be taken when these conditions are detected.
port	A connection through which a device is attached to an I/O bus or to the storage network, or the representation of this physical connection to the link hardware.
provisioning	The set of activities by which a user allocates storage to hosts and applications, for example creating LUNs in an array, setting up zoning between a host and an array, and giving the server access to the storage.
RAID	Redundant Array of Independent Disks. A set of techniques for managing multiple disks for cost, data availability, and performance. See also mirroringstriping

replication	The synchronization of data between systems where shared storage is not feasible. The systems that are copied may be in local backup clusters or remote failover sites. The major advantage of replication, when compared to traditional backup methods, is that current data is continuously available.
resource	Any of the individual components that work together to provide services on a network. A resource may be a physical component such as a storage array or a switch, a software component such as Oracle8i or a Web server, or a configuration component such as an IP address or mounted file system.
resource type	A way of classifying resources in a cluster. Each resource is identified by its name and its resource type. Symantec Cluster Server includes a set of predefined resource types for storage, networking, and application services.
router	A device that connects two segments of a storage network and determines the optimal path along which traffic should be forwarded. Also gateway. See also bridge
Rule Manager	See Action Agent
SAN	Acronym for "storage area network." A network linking servers or workstations to devices, typically over Fibre Channel, a versatile, high-speed transport. The storage area network (SAN) model places storage on its own dedicated network, removing data storage from both the server-to-disk SCSI bus and the main user network. The SAN includes one or more hosts that provide a point of interface with LAN users, as well as (in the case of large SANs) one or more fabric switches and SAN hubs to accommodate a large number of storage devices.
SCSI	Small Computer Systems Interface. A hardware interface that allows for the connection of multiple peripheral devices to a single expansion board that plugs into the computer. The interface is widely used to connect personal computers to peripheral devices such as disk and media drives.
seeding	A technique used to protect a cluster from a preexisting network partition. By default, when a system comes up, it is not seeded. Systems can be seeded automatically or manually. Only systems that have been seeded can run VCS. Systems are seeded automatically only when an unseeded system communicates with a seeded system or when all systems in the cluster are unseeded and able to communicate with each other. See network partition
service group	A collection of resources working together to provide application services to clients. It typically includes multiple resources, hardware- and software-based, working together to provide a single service.
service group dependency	A mechanism by which two service groups can be linked by a dependency rule, similar to the way resources are linked.

SF Manager Console	See Storage Foundation Management Console
shared storage	Storage devices that are connected to and used by two or more systems.
slot	An opening in a computer or other network device into which a printed circuit board can be inserted, adding capability to the device. Also expansion slot.
SMTP	Simple Mail Transfer Protocol, a commonly used protocol for sending email messages between servers.
SnapMirror	A method of mirroring volumes and qtrees on NetApp unified storage devices. With SnapMirror, a user can schedule or initiate data transfers, request information about transfers, update a mirror, and manage mirrors. See mirroring
snapshot	A point-in-time image of a volume or file system that can be used as a backup.
SNMP	The Simple Network Management Protocol for Internet network management and communications used to promote interoperability. SNMP depends on cooperating systems that must adhere to a common framework and a common language or protocol.
Storage Foundation Manager Console	A graphical user interface that displays reports and other information for users of the SF Manager and other Storage Foundation products through a standard Web browser. For users of the SF Manager, the Console provides a central point to display and manage storage resources, create and modify policies, provision storage, administer access control, and view reports.
striping	A layout technique that spreads data across several physical disks by mapping the data to successive media, known as stripes, in a cyclic pattern. Also RAID Level 0.
subdisk	In storage media managed by Veritas Volume Manager (VxVM), a set of contiguous disk blocks used for allocating disk space. A VxVM disk can be divided into one or more subdisks, each one representing a specific portion of the disk. Each portion is mapped to a specific region of a physical disk. See also plex volume
switch	A network device to which nodes attach and which provides high-speed switching of node connections via link-level addressing.
system	The physical hardware on which data and applications reside, and the connections between them.
tool	A prepackaged workflow shipped with Storage Foundation Manager for performing tasks that otherwise would require multiple operations in multiple locations. Two examples of solutions are migrating disk groups from one host to another and storing, maintaining, and implementing storage tiers by creating and executing file placement policies.

topology	The physical or logical arrangement of resources on the storage network and the connections between them.
UDID	An alternative disk identifier used internally by some components in the Storage Foundation products, for example, Veritas Volume Manager (VxVM) command-line interfaces. See also VDID
unallocated storage	LUNs that have not yet been allocated. A LUN is considered allocated when a host operating system has written a device handle for the LUN (in other words, claimed the LUN) or when the array has masked the LUN to a specific target. Contrast with allocated storage
unclaimed storage	Storage that has been allocated to hosts whose operating systems have not yet written device handles. This is usually wasted storage. Contrast with claimed storage
unconfigured storage	Physical storage that has yet to be formatted. Contrast with configured storage
unused storage	Storage to which data has not been written. Contrast with used storage
used storage	The portion of storage allocated to a file system or database to which data has been written, expressed as a quantity (such as 10 GB). Contrast with unused storage
VCS	See Veritas Cluster Server (VCS)
VDID	A unique disk identifier. See also UDID
VEA	See Veritas Enterprise Administrator (VEA)
Veritas Authentication Service (VAS)	A component of the Veritas Security Services (VxSS) that is used by the Storage Foundation offerings to provide user authentication. VAS is a set of processes and runtime libraries that enables users to log on to multiple Symantec products with one logon.
Veritas Cluster Server (VCS)	An open systems clustering solution designed to eliminate planned and unplanned downtime, simplify server consolidation, and allow the effective management of a wide range of applications in multiplatform environments.
Veritas Cluster Server cluster	A cluster consisting of multiple systems connected in various combinations to shared storage devices. Veritas Cluster Server monitors and controls applications running in the cluster and can restart applications in response to a variety of hardware or software faults. A cluster is defined as all systems with the same

cluster identification and connected via a set of redundant heartbeat networks. Clusters can have from one to 32 member systems, or nodes.

Veritas Cluster Server service group	A set of resources working together to provide application services to clients. For example, a Web application service group might consist of: disk groups on which the Web pages to be served are stored; a volume built in the disk group; a file system using the volume; a database whose table spaces are files and whose rows contain page pointers; the network interface card or cards used to export the Web service; one or more IP addresses associated with the network card(s); the application program and associated code libraries. Veritas Cluster Server performs administrative operations on resources, including starting, stopping, restarting and monitoring at the service group level.
Veritas Enterprise Administrator (VEA)	A Java-based graphical user interface monitoring and managing legacy (Storage Foundation 4.x) hosts in a single-host (standalone) management environment. The Enterprise Administrator interface provides an alternative to the browser-based SF Manager Console.
Veritas File System (VxFS)	A component of the Veritas Storage Foundation product suite that provides high performance and online management capabilities to facilitate the creation and maintenance of file systems. A file system is a collection of directories organized into a structure that enables you to locate and store files.
Veritas Storage Foundation Manager	A single, centralized management application with which administrators and operators can monitor, visualize, and manage their Storage Foundation products and generate reports about storage resources.
Veritas Volume Replicator (VVR)	A data replication tool designed to contribute to an effective disaster recovery plan. VVR is a feature of Veritas Volume Manager (VxVM).
Veritas Volume Manager (VxVM)	A Symantec product installed on storage clients that enables management of physical disks as logical devices. VxVM enhances data storage management by controlling space allocation, performance, data availability, device installation, and system monitoring of private and shared systems.
virtual IP address	A unique IP address associated with a VCS cluster. This address can be used on any system in the cluster, along with other resources in the VCS cluster service group. A virtual IP address is different from a system's base IP address, which corresponds to the system's host name. See also IP address
virtualization	Representing one or more objects, services, or functions as a single abstract entity so that they can be managed or acted on collectively. An example of virtualization is the creation of a virtual fabric from a switch and associated storage resources as a means of controlling access and increasing scalability in the storage network.

volume	<p>In storage media managed by Veritas Volume Manager, a virtual disk made up of a portion or portions of one or more physical disks and representing an addressable range of disk blocks. A volume appears to applications, databases, and file systems like a physical disk device, but it does not have the physical limitations of a physical disk device. A volume consists of one or more plexes, each holding a copy of the selected data in the volume. Due to its virtual nature, a volume is not restricted to a particular disk or a specific area of a disk.</p> <p>See also plex subdisk</p>
VVR	See Veritas Volume Replicator (VVR)
VxVM	See Veritas Volume Manager (VxVM)
World Wide Name (WWN)	A registered, 64-bit, unique identifier that is assigned to nodes and ports.

Index

D

DMP

identifying active nodes 11

H

hosts

identifying active 11

P

ports

maintenance 11

R

resources

identifying active 11

S

support

commenting on documentation 32

V

Volume Manager (VxVM)

identifying active objects 11