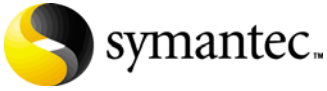
Veritas Storage Foundation™ and High Availability Solutions Management Pack Guide for Microsoft Operations Manager 2005

Windows Server 2003

5.1 Service Pack 1



Veritas Storage Foundation and High Availability Solutions Management Pack Guide for Microsoft Operations Manager 2005

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: 5.1. Service Pack 1

Document version: 5.1.SP1.0

Legal Notice

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:

http://www.symantec.com/business/support/index.jsp

Contacting Technical Support

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

http://www.symantec.com/business/support/contact_techsupp_static.jsp

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:

http://customercare.symantec.com

Customer service

Customer service information is available at the following URL:

http://customercare.symantec.com

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	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

Section 1

Introduction

This section includes the following chapters:

Chapter 1

Introducing Veritas Storage Foundation and High Availability Solutions support for MOM 2005

About this guide

This guide contains information on the following management packs:

- Veritas Storage Foundation for Windows (SFW) Management Pack
- Veritas Cluster Server (VCS) Management Pack

Symantec provides two separate Management Packs for Microsoft Operations Manager (MOM) 2005, one for SFW and the other for VCS. As required, you can choose to use only the SFW MOM pack or both SFW and VCS Management Packs. You will need to deploy two separate .akm files to enable MOM 2005 monitoring for SFW and VCS. The .akm files are part of the product package but you will need to import them separately.

For specific information about MOM 2005, see the MOM 2005 product documentation.

How this guide is organized

This guide explains how to use the SFW and the VCS Management Packs to monitor specific components.

You can read about deployment options of the SFW and VCS Management Pack. You will also learn how the SFW Management Pack monitors the performance using different views and how the VCS Management pack generates reports.

See the following sections for more information:

- Section 2, “Veritas Storage Foundation for Windows (SFW) MOM pack” on page 15
- Section 3, “Veritas Cluster Server (VCS) MOM Pack” on page 83

Section 2

Veritas Storage Foundation for Windows (SFW) MOM pack

This section contains the following chapters:

Chapter 2

Overview: Veritas Storage Foundations for Windows Management Pack

About the SFW Management Pack for MOM

The Veritas Storage Foundation for Windows Microsoft Operations Manager (MOM) 2005 Management Pack monitors events placed in the Windows event logs and selected perfmon counters. With its set of alerts, the SFW Management Pack can help you monitor the events generated by the SFW components such as disks, disk groups, and volumes. The event log displays the following message types: errors, warnings, and informational messages.

The SFW Management Pack alerts are designed to notify you of critical events requiring attention. A public view of the status of Storage Foundation for Windows (SFW) is also provided. This guide also includes the set of rules that indicate the health of SFW components.

This guide is especially intended for the MOM administrator, and provides information about how the SFW Management Pack is used for event monitoring.

Note: The MOM console display for the Management Pack is localized in all languages supported by Veritas Storage Foundation 5.1 for Windows.

SFW Management Pack processing rule groups

This section lists the processing rule groups which are used for monitoring the specific components. Each rule group consists of a set of messages that are used to monitor the specific components.

SFW processing rule groups

The SFW Management Pack supports the following processing rule groups.

Table 2-1 Processing Rule Groups

Rule Group	Description
Disks, Disk Groups, and Volumes	Monitors the operational status of dynamic disks, volumes, and disk groups. Also included is the status of SCSI reservations of cluster and private disk groups. Performance information for dynamic disks and volumes may be enabled.
Dynamic Multi-pathing	Monitors the status of arrays managed by Dynamic Multi-pathing (DMP) Array Support Libraries (ASLs) and DMP Device Specific Modules (DSMs).
FlashSnap	Monitors the FlashSnap operations: Snap Start, Snap Shot, and Snap Back.
Licensing	Monitors when an invalid, duplicate, or expired license situation occurs.
Volume Replicator (VVR)	Monitors the operation of Veritas Volume Replicator RDS, RVG, and RLINK objects. Performance information about VVR memory usage and remote host replication status is also present.
VxCache	Monitors the status of VxCache memory management and I/O operations.

About SFW Management Pack Public View

Public views enable you to view the hardware and software configuration and status data related to the application. The top-level public view for SFW is called Veritas Storage Foundation for Windows. It contains a folder for each of the processing rule groups described in the section “SFW processing rule groups” on page 19. Each folder contains an alert view and an event view. Depending on the rule and the alert that has been set for an event, an appropriate alert is generated when the event is received on the MOM server.

The following table indicates the alert categories for the Management Packs.

Table 2-2 Alert Categories

Severity Level	Definition
SUCCESS	Successful completion of an operation
INFORMATION	The application raises an informational event
WARNING	Indication of potential future problem, or lower priority issue does not require any immediate action.
ERROR	The application is experiencing transient errors that requires attention, but does not require action immediately and is not an indication of imminent failure.
CRITICAL ERROR	The application is experiencing a serious problem that requires immediate attention. The application requires action to correct an error condition.

In general, the Management Packs have the following default settings for events and alerts.

Table 2-3 Default Settings

Alert	Default Setting
SUCCESS	event rule disabled
INFORMATION	event rule disabled
WARNING	event enabled with alert enabled
ERROR	event enabled with alert enabled
CRITICAL ERROR	event enabled with alert enabled

Note: There are some exceptions to these settings in which lower severity level events are enabled, and for which alerts might also be enabled.

The Management Pack does not include a notification group for automatic alerts by email. If email alerts are required, you must add the alert processing rules manually.

The collection of dynamic disk and volume perfmon counters is disabled by default. Data collection is not limited to a single SFW server, disk, or volume.

Infact, data is collected for all dynamic disks or volumes on all SFW servers managed by the MOM server. If the management domain includes SFW servers with a large number of dynamic disks and volumes, data collection should only be enabled for limited time periods so as not to overpopulate the MOM database.

SFW Management Pack Public Views

The Management Pack provides the following folders under Monitoring views.

Table 2-4 Folders under Monitoring Views

Folders	Description
Alert View for all SFW 4.3 and 5.x Servers	Active alerts for all SFW 4.3x and 5.x SFW servers.
Event View for all SFW 4.3 and 5.x Servers	Events received by Ops Mgr for all SFW 4.3x and 5.x SFW servers.
Performance	Active performance counters for all SFW 4.3x and 5.x servers.
State View for all SFW 4.3 and 5.x Servers	State view for all SFW.4.3x and 5.x servers.
State View for Servers with DMP DSM Option	State view for all SFW servers with installed DMP DSM option.
State View for Servers with MSCS Option	State view for all SFW servers where MSCS is installed.
State View for Servers with Volume Replicator (VVR) Option	State view for all SFW servers with installed VVR option.

Chapter 3

Deploying the SFW Management Pack

About deploying the SFW Management Pack

This guide describes how to deploy and configure the SFW Management Pack into your existing Microsoft Operations Manager (MOM) 2005 environment.

Verifying the compatibility considerations

The SFW Management Pack is compatible with:

- Microsoft Operations Manager 2005 with Service Pack (SP) 1

Note: The MOM console display for the Management Pack is localized in all languages supported by Veritas Storage Foundation 5.1 for Windows.

Supported software and operating systems

This version of the SFW Management Pack is supported on VSFW 4.3 and later versions, on Windows Server 2003.

Prerequisite

Verify that MOM 2005 infrastructure has been set up. For details, see the appropriate MOM documentation.

Deploying the Management Pack

This section provides information about enabling the SFW Management Pack to monitor the events.

Importing the SFW Management Pack

From the MOM 2005 SP1 Administrator Console import the `SFW_MOM2005.akm` to deploy the SFW Management Pack.

Updating the SFW Management Pack

This section provides information about upgrading the SFW MOM 2005 pack when the SFW 4.3 MOM Pack or the SFW 5.0 MOM Pack is already present on your setup.

SFW 4.3 MOM Pack or SFW 5.0 MOM Pack is present and has been modified

If you have the SFW 4.3 MOM Pack or the SFW 5.0 MOM Pack already installed on your setup and if you have modified the Management Pack to include Symantec knowledge base information, then do the following:

1. Open the Management Pack Operator Console.
2. Right-click the SFW MOM pack public view, `Veritas Storage Foundation by Symantec`, and select **Delete** from the context menu.
3. Open the Management Pack Import/Export Wizard.
4. Navigate the wizard pages and on the Select Management Packs panel, select select **Update existing Management Pack**, and check the **Back up existing Management Pack** checkbox.

SFW 4.3 MOM Pack or SFW 5.0 MOM Pack is present and has not been modified

If you have the SFW 4.3 MOM Pack or the SFW 5.0 MOM Pack already installed on your setup and if you have not modified the Management Pack, then do the following:

1. Open the Management Pack Operator Console.
2. Right-click the SFW MOM pack public view, `Veritas Storage Foundation by Symantec`, and select **Delete** from the context menu.
3. Open the Management Pack Import/Export Wizard.

4 Navigate the wizard pages and on the Select Management Packs panel select **Replace existing Management Pack**. In this case you do not need to select the option to backup the existing Management Pack.

Technical reference

Registry

The SFW Management Pack collects the following attributes for computers:

Table 3-1 Registry keys referenced by SFW management pack

Attribute Name	Registry Path
Veritas Storage Foundation for Windows Version **Attribute Type**: Registry value	`SOFTWARE\VERITAS\VxSvc\CurrentVersion\VolumeManager\Version`
Veritas Storage Foundation by Symantec Version **Attribute Type**: Registry value	`SOFTWARE\VERITAS\VxSvc\CurrentVersion\VolumeManager\Version`
Veritas Storage Foundation by Symantec 64-bit Version **Attribute Type**: Registry value	`SOFTWARE\Wow6432Node\Veritas\VxSvc\CurrentVersion\VolumeManager\Version`
Veritas Storage Foundation 5.0 Servers with VVR Option **Attribute Type**: Registry value	`SOFTWARE\VERITAS\VRTSobc\pal33\Agents\StorageAgent\Providers\vvr`
Veritas Storage Foundation VVR 5.0 64-bit Servers with VVR Option **Attribute Type**: Registry value	`SOFTWARE\Wow6432Node\Veritas\VRTSobc\pal33\Agents\StorageAgent\Providers\vvr`
Veritas Storage Foundation 4.3 Servers with VVR Option **Attribute Type**: Registry value	Type: Registry value `SOFTWARE\VERITAS\VxSvc\CurrentVersion\Providers\vvr`

Table 3-1 Registry keys referenced by SFW management pack (Continued)

Attribute Name	Registry Path
Veritas Storage Foundation 4.3 64-bit Servers with VVR Option **Attribute Type**: Registry value	Type: Registry value `SOFTWARE\Wow6432Node\VERITAS\VxSvc\CurrentVersion\Providers\vvr`
Veritas Storage Foundation 5.0 Servers with DMP DSM Option **Attribute Type**: Registry value	Type: Registry value `SOFTWARE\VERITAS\VRTSobc\pal33\Agents\StorageAgent\Providers\mpioprov`
Veritas Storage Foundation 5.0 64-bit Servers with DMP DSM Option **Attribute Type**: Registry value	Type: Registry value `SOFTWARE\Wow6432Node\Veritas\VRTSobc\pal33\Agents\StorageAgent\Providers\mpioprov`
Veritas Storage Foundation Servers with MSCS VMDG Resource Type **Attribute Type**: Registry value	Type: Registry value `Cluster\ResourceTypes\Volume Manager Disk Group`

Notification Groups

The Management Pack does not include a notification group.

Chapter 4

Monitoring and reporting

About monitoring and reporting in SFW Management Pack

This chapter describes how you can monitor the Veritas Storage Foundation for Windows using the available views. The views supported by the SFW Management packs enable you to monitor the health of the different components within the managed environment. You can then use the reporting functionality to generate the required reports.

Monitoring nodes using views

The views supported by the SFW Management pack are available through the Operator Console. These views enable you to assess the state of the required node within the managed environment. The operator console supports the following views:

- Alert view
- State view
- Event view
- Diagram view

Alert view

The Alert View provides a list of issues requiring action and the current state and severity of each alert. It indicates whether the alerts have been acknowledged, escalated, or resolved, and also whether a Service Level Agreement has been breached.

State view

The State view provides a real-time, consolidated look at the health of the system within the managed environment, highlighting the systems that require attention.

SFW State view

The SFW state view displays the state of each of the predefined groups. The name of each of the state view and the corresponding details are as follows:

- **State View for all SFW 4.3 and 5.x Servers**
  Displays the state view for all the servers in the Veritas Storage Foundation Servers Computer Group that have open alerts.

- **State View for Servers with DMP DSM Option**
  Displays the state view for all the servers in the Veritas Storage Foundation 5.x for Windows by Symantec Servers with DMP DSM Option Computer Group that have open alerts.

The state view displays the state of each service group on the current node, along with the state of the IP and VMDg resources. If a service group has multiple IP address or VMDg resources, then only the information about the instance that is in the worst state is displayed in the state view.

The SFW rule groups use some scripts to collect the required performance data or objects data. Following is the script that is used by SFW rule groups:

- `Veritas SFW DMP DSM path performance data`—Collects the Dynamic Multi-pathing performance data for Veritas Storage Foundation and provides this information to the MOM server.

VVR State view

The VVR state view, **State View for all SFW 4.3 and 5.x Servers with VVR option,** displays the data access and replication state for all the servers having open alerts in the Veritas Volume Replicator (VVR) Computer Group.

The Veritas Volume Replicator rule groups use scripts to collect the required VVR performance data or objects data. To enable the scripts to fetch the VVR information from the servers, make sure that the `vxvm` service is running on all the nodes. The following scripts are used by the VVR state view:

- `VVR Objects Discovery Data`—Collects the VVR objects information and provides this information to the MOM server. By default, this script collects data every fifteen minutes.
- `VVR Object State Monitoring Data`—Collects the VVR objects and state monitoring information and provides this information to the MOM server. By default, this script collects data every nine minutes.

State of data access to volumes under replication

The state of data access is monitored with the help of the RVG state information collected by the scripts mentioned earlier and flags information gathered by the

vxprint command. Each state is represented by an icon to indicate the severity of the alert.

State Icon	Alert Severity	RVG State and flags in vxprint	Description
	Success	Active	Data access enabled
	Error	Clean	Data access disabled
	Critical Error	Fail	I/O error

State of replication across VVR servers

The state of data replication is governed by the RLINKs that exist between the primary and secondary sites. This state is monitored with the help of the RLINK state information gathered by the scripts and flag information that is gathered by the vxprint command output. Each RLINK is associated with a unique remote host. Hence, the number of instances displayed in the state view is equal to the number of RLINKs associated with the RVG. If there are no associated RLINKs, then the replication state is not shown, only the data access state is shown for the RVG. The naming scheme used for representing the VVR objects in the state view is as follows:

```
Diskgroup=<DG>, RVG=<rvg>, Role={prmary | secondary} |
acting_secondary}, RemoteHost=<RlinkRemoteHost>
```

Note: Each state is represented by an icon to indicate the severity of the alert. However, the alert severity for RLINK from one secondary to another is represented by the information icon ⓘ regardless of the RLINK and flags state.

Icon representing state	Alert Severity	RLINK state and flags in vxprint	Description
	Success	Attached, connected	Replication is active

Icon representing state	Alert Severity	RLINK state and flags in vxprint	Description
	Warning	Attached, disconnected	Replication is activating
	Warning	Pause	Replication is paused
	Error	Detached	Replication is inactive
	Critical Error	Fail	I/O error on Secondary

Event view

The Event view provides a list of events that have occurred on managed servers, a description of each event, and the source of the problem.

Performance view

The Performance View displays the tabulated information of SFW and VVR counters in the right-pane details view. You can select the required counters and click **Draw Graph** to view the graphical view. The Performance View displays performance data only for the DMP and VVR.

DMP DSM performance data counters

A new event rule called Get MPIO Performance Data has been added to the Dynamic Multi-pathing\Veritas DMP DSMs (MPIO Device Specific Modules) rule group for the MOM 2005 Pack. Get MPIO Performance Data and its data provider is a timed response which triggers an event every 15 minutes. The event rule is disabled by default.

When enabled, the event rule executes a vbscript on the MOM 2005 server. The vbscript executes `vxdmpadm.exe` on the SFW agent-managed computers where the DMP DSM option is installed. It uses a new vxdmpadm option called `allperf` , which returns a set of comma-separated values:

```
counter name, path, device, array, counter value
```

For each SFW server on which the vbscript is run, the script creates a set of performance objects on the MOM 2005 server with counter names in the format `counter name\path\device` . The counters are automatically added to the

MOM server's performance counter list for the SFW computer from which the data is gathered.

The data collected is a set of counters on a per second basis. There is no need to increase the frequency of collection.

Chapter 5

SFW monitoring rules

About the SFW monitoring rules

This chapter lists the monitoring rules for the various SFW modules. The monitoring rules consist of event processing rules and alert processing rules.

Disks, Disk Groups, and Volumes monitoring rules

Disks, Disk Groups, and Volumes (DDGV) rules are located in the Veritas Storage Foundation for Windows folder.

Table 5-1 lists the Disks, Disk Groups, and Volumes rules included in the SFW Management Pack.

Table 5-1 DDGV event rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
700	vmperf	Statistics collection failed.	Error	Yes	No
1	vxboot	Vxboot error.	Error	Yes	Yes
2	vxboot	No mount point. Failed to start volume.	Error	Yes	Yes
3	vxboot	Failed to start volume.	Error	Yes	Yes
4	vxboot	Failed to upgrade selected disks.	Error	Yes	Yes
5	vxboot	Disk group failed. All volumes in the disk group are unavailable.	Error	Yes	Yes
6	vxboot	Failed to auto-import disk group. All volumes in the disk group are unavailable.	Error	Yes	Yes
7	vxboot	Volume started in failed redundancy mode (no mountpoint).	Warning	Yes	Yes
8	vxboot	Volume started in failed redundancy mode.	Warning	Yes	Yes
8	vxboot	VVR objects discovery	Unknown	Yes	No

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
9	vxboot	RAID-5 log is used for fast recovery of volume after system crash.	Information	No	No
10	vxboot	RAID-5 log is used for fast recovery of volume after system crash.	Information	No	No
11	vxboot	DRL is used for fast recovery of volume after system crash.	Information	No	No
12	vxboot	DRL is used for fast recovery of volume after system crash.	Information	No	No
13	vxboot	RAID-5 log failed for volume. Full resynchronization is required.	Information	Yes	No
14	vxboot	RAID-5 log failure. Full resynchronization is required.	Warning	Yes	No
15	vxboot	DRL failed for volume. Full resynchronization is required.	Warning	Yes	Yes
16	vxboot	DRL failure for volume. Full resynchronization is required.	Warning	Yes	No
17	vxboot	Volume was not shut down cleanly. Resynchronization is required.	Warning	Yes	No
18	vxboot	Volume was not resynchronized during previous shutdown. Resynchronization task will be resumed.	Information	Yes	Yes

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
19	vxboot	One or more disks are missing during import of disk group.	Warning	Yes	No
20	vxboot	Volume has duplicate GUID.	Warning	Yes	No
21	vxboot	GUID of volume was changed.	Warning	Yes	No
1	vxio	Device received spurious close request.	Information	No	No
2	vxio	Failed to log DRL volume detach.	Error	Yes	Yes
3	vxio	DRL volume is detached.	Information	No	No
4	vxio	Error on volume.	Error	Yes	Yes
5	vxio	Object detached from volume.	Information	No	No
6	vxio	Overlapping mirror detached from volume.	Information	No	No
7	vxio	Kernel log full, object detached.	Information	No	No
8	vxio	Kernel log update failed, object detached.	Error	Yes	No
9	vxio	Detaching RAID-5 object.	Information	No	No
10	vxio	Object detached from RAID-5 volume.	Information	No	No
11	vxio	RAID-5 volume entering degraded mode operation.	Warning	Yes	No
12	vxio	Double failure condition detected on RAID-5 volume.	Warning	Yes	Yes
13	vxio	Failure during RAID-5 logging operation.	Error	Yes	Yes

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
14	vxio	Log object detached from RAID-5 volume.	Error	Yes	No
15	vxio	Check_ilocks: stranded ilock.	Warning	Yes	No
16	vxio	Check_ilocks: overlapping ilocks.	Warning	Yes	No
17	vxio	Illegal vminor encountered.	Warning	Yes	No
18	vxio	Uncorrectable error.	Error	Yes	No
19	vxio	Uncorrectable error on block.	Error	Yes	No
20	vxio	Kernel error, cannot open disk.	Error	Yes	No
21	vxio	Unexpected status on disk close.	Warning	Yes	No
22	vxio	Corrected read error on volume mirror object.	Information	No	No
23	vxio	Reassigning bad block number on disk.	Information	No	No
24	vxio	Successfully reassigned bad block(s) on disk.	Information	No	No
25	vxio	Failed to reassign bad block(s) on disk.	Warning	Yes	No
26	vxio	Found a bad block on disk.	Information	No	No
27	vxio	Corrected a read error during RAID5 initialization.	Information	No	No
28	vxio	Failed to recover a read error during RAID5 initialization.	Warning	Yes	No
29	vxio	Read error.	Critical Error	Yes	Yes

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
30	vxio	Write error.	Critical Error	Yes	Yes
31	vxio	Write error due to disk removal.	Error	Yes	No
32	vxio	Read error due to disk removal.	Error	Yes	No
33	vxio	Disk is disabled by PnP.	Information	No	No
34	vxio	Disk is re-onlined by PnP.	Information	No	No
35	vxio	Uncorrectable disk read error.	Warning	Yes	No
36	vxio	Uncorrectable read error.	Warning	Yes	No
37	vxio	Uncorrectable disk write error.	Warning	Yes	No
38	vxio	Uncorrectable write error.	Warning	Yes	No
39	vxio	Invalid name for vxio tunable.	Error	Yes	No
40	vxio	Vxio tunable out of range. It has been reset.	Error	Yes	No
41	vxio	Cluster or private disk group has lost access to a majority of its disks. Its reservation thread has been stopped.	Critical Error	Yes	Yes
48	vxio	Bus reset command sent to SCSI port.	Information	No	No
49	vxio	Volume still open during system shutdown.	Warning	Yes	No
50	vxio	Reservation thread stopped for cluster disk group. Cluster software may not be available.	Critical Error	Yes	Yes

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
51	vxio	Vxio tunable value is less than the allocated value.	Information	No	No
52	vxio	Reservation refresh has been suspended.	Error	Yes	Yes
53	vxio	Reservation refresh has been resumed.	Information	Yes	Yes
800	VxSvc_disk	Write disk signature succeeded.	Success	No	No
801	VxSvc_disk	Write disk signature failed.	Error	Yes	No
803	VxSvc_disk	Convert disk succeeded.	Success	No	No
804	VxSvc_disk	Convert disk failed.	Error	Yes	No
8014	VxSvc_disk	S.M.A.R.T. predicts failure on a device.	Warning	Yes	No
807	VxSvc_fsys	Volume capacity reached error condition.	Error	Yes	Yes
810	VxSvc_fsys	Volume free space has reached the warning threshold.	Warning	Yes	No
912	VxSvc_fsys	Volume successfully formatted.	Success	No	No
915	VxSvc_fsys	Format volume failed.	Error	Yes	No
919	VxSvc_fsys	Extend volume file system succeeded.	Success	Yes	Yes
922	VxSvc_fsys	Extend volume file system failed.	Error	Yes	No
926	VxSvc_fsys	Change volume label succeeded.	Success	No	No
929	VxSvc_fsys	Change volume label failed.	Error	Yes	No
933	VxSvc_fsys	Check volume file system succeeded.	Success	No	No

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
936	VxSvc_fsys	Check volume file system failed.	Error	Yes	No
940	VxSvc_fsys	Cancel formatting volume succeeded.	Information	No	No
944	VxSvc_fsys	Format failed because volume size is too small.	Error	Yes	No
948	VxSvc_fsys	Format failed because volume size is too big.	Error	Yes	No
952	VxSvc_fsys	Format failed because the allocation size is too small.	Error	Yes	No
956	VxSvc_fsys	Format failed because the allocation size is too big.	Error	Yes	No
968	VxSvc_fsys	Successfully shrunk file system on a volume.	Information	Yes	No
972	VxSvc_fsys	Failed to shrink file system on a volume.	Error	Yes	Yes
800	VxSvc_ftdisk	Create partition succeeded.	Success	No	No
801	VxSvc_ftdisk	Create partition failed.	Error	Yes	No
802	VxSvc_ftdisk	Delete partition succeeded.	Success	No	No
803	VxSvc_ftdisk	Delete partition failed.	Error	Yes	No
804	VxSvc_ftdisk	Mark partition active succeeded.	Success	No	No
805	VxSvc_ftdisk	Mark partition active failed.	Error	Yes	No
806	VxSvc_ftdisk	Resize partition succeeded.	Success	No	No
807	VxSvc_ftdisk	Resize partition failed.	Error	Yes	No
10120	VxSvc_ftdisk	Automatic BOOT.INI update succeeded.	Information	No	No

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
10125	VxSvc_ftdisk	Automatic BOOT.INI update failed.	Error	Yes	No
800	VxSvc_mount	Add drive letter succeeded.	Success	No	No
801	VxSvc_mount	Add drive letter failed.	Error	Yes	No
802	VxSvc_mount	Remove drive letter succeeded.	Success	No	No
803	VxSvc_mount	Remove drive letter failed.	Error	Yes	No
804	VxSvc_mount	Add mount path succeeded.	Success	No	No
805	VxSvc_mount	Add mount path failed.	Error	Yes	No
806	VxSvc_mount	Remove mount path succeeded.	Success	No	No
807	VxSvc_mount	Remove mount path failed.	Error	Yes	No
800	VxSvc_pnp	Device arrived.	Information	No	No
801	VxSvc_pnp	Device removed.	Warning	Yes	No
801	VxSvc_scheduler	Failed to create new schedule.	Error	Yes	Yes
803	VxSvc_scheduler	Failed to delete schedule.	Error	Yes	Yes
805	VxSvc_scheduler	Modify schedule failed.	Error	Yes	Yes
807	VxSvc_scheduler	Launch task failed.	Error	Yes	Yes
809	VxSvc_scheduler	Refresh schedules failed.	Error	Yes	Yes
703	VxSvc_vxvm	Create volume succeeded.	Success	No	No
704	VxSvc_vxvm	Create volume failed.	Error	Yes	No
705	VxSvc_vxvm	Delete volume succeeded.	Success	No	No

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
706	VxSvc_vxvm	Delete volume failed.	Error	Yes	No
711	VxSvc_vxvm	Add mirror succeeded.	Information	No	No
712	VxSvc_vxvm	Add mirror failed.	Error	Yes	No
713	VxSvc_vxvm	Remove mirror succeeded.	Success	No	No
714	VxSvc_vxvm	Remove mirror failed.	Error	Yes	No
715	VxSvc_vxvm	Break mirror succeeded.	Success	No	No
716	VxSvc_vxvm	Break mirror failed.	Error	Yes	No
717	VxSvc_vxvm	Resize volume succeeded.	Success	No	No
718	VxSvc_vxvm	Resize volume failed.	Critical Error	Yes	Yes
719	VxSvc_vxvm	Reactivate volume succeeded.	Success	No	No
720	VxSvc_vxvm	Reactivate volume failed.	Error	Yes	No
721	VxSvc_vxvm	Replace column succeeded.	Success	No	No
722	VxSvc_vxvm	Replace column failed.	Error	Yes	No
729	VxSvc_vxvm	Remove missing disk failed.	Error	Yes	No
741	VxSvc_vxvm	Remove missing disk succeeded.	Success	No	No
746	VxSvc_vxvm	Repair volume succeeded.	Success	No	No
747	VxSvc_vxvm	Repair volume failed.	Error	Yes	No
748	VxSvc_vxvm	Add log succeeded.	Success	No	No
749	VxSvc_vxvm	Add log failed.	Error	Yes	No
750	VxSvc_vxvm	Remove log succeeded.	Success	No	No
751	VxSvc_vxvm	Remove log failed.	Error	Yes	No
752	VxSvc_vxvm	Add fast resync succeeded.	Success	No	No

Table 5-1 DDGV event rules (Continued)

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
753	VxSvc_vxvm	Add fast resync failed.	Error	Yes	No
754	VxSvc_vxvm	Remove fast resync succeeded.	Success	No	No
755	VxSvc_vxvm	Remove fast resync failed.	Error	Yes	No
756	VxSvc_vxvm	Snap Start succeeded.	Success	No	No
757	VxSvc_vxvm	Snap Start failed.	Error	Yes	No
758	VxSvc_vxvm	Snap Shot succeeded.	Success	Yes	Yes
759	VxSvc_vxvm	Snap Shot failed.	Error	Yes	No
760	VxSvc_vxvm	Snap Back succeeded.	Success	Yes	Yes
761	VxSvc_vxvm	Snap Back failed.	Error	Yes	No
762	VxSvc_vxvm	Snap Clear succeeded.	Success	Yes	No
763	VxSvc_vxvm	Snap Clear failed.	Error	Yes	No
764	VxSvc_vxvm	Snap Abort succeeded.	Success	No	Yes
765	VxSvc_vxvm	Snap Abort failed.	Error	Yes	No
766	VxSvc_vxvm	Split subdisk succeeded.	Success	No	No
767	VxSvc_vxvm	Split subdisk failed.	Error	Yes	No
768	VxSvc_vxvm	Join subdisk succeeded.	Success	No	No
769	VxSvc_vxvm	Join subdisk failed.	Error	Yes	No
770	VxSvc_vxvm	Import dynamic disk group succeeded.	Success	No	No
771	VxSvc_vxvm	Import dynamic disk group failed.	Error	Yes	No
772	VxSvc_vxvm	Deport dynamic disk group succeeded.	Success	No	No
773	VxSvc_vxvm	Deport dynamic disk group failed.	Error	Yes	No
774	VxSvc_vxvm	Split dynamic disk group succeeded.	Success	Yes	Yes