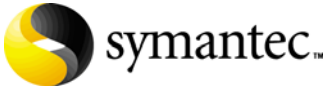
Veritas Storage Foundation™ and High Availability Solutions Management Pack Guide for Microsoft System Center Operations Manager 2007

Windows Server 2003
Windows Server 2008

5.1 Service Pack 1



Veritas Storage Foundation for Windows Management Pack Guide for Microsoft System Center Operations Manager 2007

Product version: 5.1. Service Pack 1

Document version: 5.1.SP1.0

Legal Notice

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:

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

Chapter 1

Overview: Veritas Storage Foundation for Windows Management Pack

The Veritas Storage Foundation for Windows Management Pack for Microsoft System Center Operations Manager 2007 monitors events placed in the Windows event logs and selected performance counters. With its set of alerts, the SFW Management Pack can help you monitor the events and performance counters 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 intended for the Microsoft System Center Operations Manager 2007 (Ops Mgr 2007) administrator and provides information about how the SFW Management Pack is used for event monitoring.

This guide describes how to deploy and configure the SFW Management Pack in your Ops Mgr 2007 environment. Symantec provides you with an .mp file to enable Ops Mgr 2007 monitoring for SFW. The .mp file must be imported into Ops Mgr 2007 to enable monitoring.

For specific information about Ops Mgr 2007, see the Microsoft System Center Operations Manager 2007 product documentation.

Note: The SFW Management Pack is delivered in English only. However, event text that comes from a localized server does appear in the localized language.

SFW Management Pack Event Rules

This section lists the event rule categories which are used for monitoring the specific components. Each of the categories consist of a set of messages that are used to monitor the specific components.

SFW Event Rule Categories

The SFW Management Pack supports the following event rule categories.

Table 1-1 Event Rule Categories

Event Rule Category	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 Veritas Storage Foundation by Symantec Monitoring

Monitoring views enable you to view the hardware and software configuration and status data related to the application. The top-level view for SFW is called Veritas Storage Foundation by Symantec. It contains a folder for each of the categories of rules described in the section “SFW Management Pack Monitoring” on page 12. Each folder contains alerts and events. 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 Ops Mgr server.

The following table indicates the alert categories for the SFW Management Pack.

Table 1-2 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 Pack has the following default settings for events and alerts.

Table 1-3 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 SFW 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 performance counters is disabled by default. Data collection cannot be limited to a single SFW server, disk, or volume; rather, data is collected for all dynamic disks or volumes on all SFW servers managed by the Ops Mgr 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 Ops Mgr database.

SFW Management Pack Monitoring

The SFW Management Pack provides the following folders under Monitoring views.

Table 1-4 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 2

Deploying the SFW Management Pack

This guide describes how to deploy and configure the SFW Management Pack in your existing Microsoft System Center Operations Manager 2007 environment.

This version of the SFW Management Pack is supported on SFW 4.3.x, SFW 5.0, SFW 5.1, and later versions running on Windows Server 2003 and Windows Server 2008. The SFW Management Pack is compatible with Microsoft System Center Operations Manager 2007 SP1 and Microsoft System Center Operations Manager 2007 R2.

Note: The SFW Management Pack is delivered in English only. However, event text that comes from a localized server does appear in the localized language.

Prerequisite

Verify that the Ops Mgr 2007 infrastructure is set up and running correctly. For more information, see the appropriate Microsoft System Center Operations Manager 2007 SP1 or Microsoft System Center Operations Manager 2007 R2 documentation.

Deploying the Management Pack

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

Importing the SFW Management Pack

The SFW Management Pack is a sealed management pack named `Symantec.SFW.mp`. A sealed management pack means that a user has the ability to make limited changes to the management pack.

To install the SFW Management Pack:

1. Open the Administration pane of the Operator Console and select **Management Packs** to display the operations available for managed packs.
2. In the right pane of the Operator Console under Actions, click on “Import Management Packs”. (You can also use the toolbar, by selecting Actions>Actions>Import Management Packs.)
   The “Select Management Packs to Import” window appears.
3. In the “Select Management Packs to Import” window, navigate to `Symantec.SFW.mp`.
4. Select `Symantec.SFW.mp` and click **Open**.
   The “Import Management Packs” window appears.
5. In the “Import Management Packs” window, select the pack “Veritas Storage Foundation for Windows by Symantec”, Version 5.1.1.0.
   Click **Import** to complete the process.

When the management pack is successfully imported, it appears in the Management Packs list.

Updating the SFW Management Pack

This section provides information about upgrading the SFW Ops Mgr 5.1.1.0 pack.

Note: Upgrading an existing SFW Microsoft Operations Manager (SFW MOM) pack to this SFW Management Pack is not supported. Also Symantec does not recommend upgrading an existing SFW MOM pack with the Microsoft conversion feature.

SFW 5.0 Ops Mgr Pack or SFW 5.1.0 Ops Mgr Pack is present and has been modified

If you have the SFW 5.0 Ops Mgr Pack or the SFW 5.1.0 Ops Mgr Pack already installed on your setup and if you have modified the Management Pack with rule overrides, then do the following:

1. Export the management pack containing the rule overrides to a backup file. (You may be exporting the default management pack or a management pack that only contains SFW rule overrides.) Save the backup file so that you can import your pack in a later step.
2. Delete the override management pack.
3. Delete the SFW management pack.
4. Import the SFW 5.1 Ops Mgr or SFW 5.1.1.0 Ops Mgr pack.
5. Import the override management pack that you exported and saved in an earlier step.

SFW 5.0 Ops Mgr Pack or SFW 5.1.0 Ops Mgr Pack is present and has not been modified

If you have the SFW 5.0 Ops Mgr Pack or the SFW 5.1.0 Ops Mgr Pack already installed on your setup and if you have not modified the Management Pack, then do the following:

1. Delete the SFW management pack.
2. Import the SFW 5.1.1.0 Ops Mgr pack.

Technical Reference

Registry

The SFW Management Pack collects the following attributes for computers:

Table 2-1

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 2-1

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`

Notification Groups

The Management Pack does not include a notification group.

Chapter 3

Monitoring and Reporting

This chapter describes how you can monitor Veritas Storage Foundation for Windows using the available views. The views supported by the SFW Management Pack enable you to monitor the health of the different components within the managed environment. Although the SFW Management Pack is sealed, you have the ability to make limited changes to the rules to customize the monitoring of components.

Locating rules

Rules are ordered differently in Ops Mgr 2007 than in earlier releases of the Microsoft Operations Manager (MOM). In Ops Mgr2007, rules appear in a large list in the Authoring pane of the Operator Console. You display the rules by selecting the Rules object under Management Pack Objects. You can narrow the scope of the rules being displayed (filter the display of the rules) by selecting View>Scope in the toolbar. In the Scope Management Pack Objects window that appears, you can select the Veritas Storage Foundation objects to limit the display to only the rules provided by the SFW Management Pack.

To locate a rule, you scroll through the list of rules or enter a search string in the **Look for** field at the top of the display. Using the **Look for** field locates all instances of the rule regardless of the SFW group that contains it.

For example, to locate particular rules for the VVR performance counters, you would refer to the table of VVR performance counters in “Volume Replicator (VVR) Performance Rules” on page 73. For the purpose of this example, assume that the rules that you are interested in all contain the string “Kbytes”. The string “Kbytes” can be used as the search string for the rules. Enter the search string in the **Look for** field and click **Find Now** to locate the rules. The search results for the VVR performance counters appear in two groups, “Veritas Storage Foundation for Windows by Symantec Servers Installation” and “Veritas Storage Foundation for Windows by Symantec Servers with VVR Option Installation”.

Enabling and disabling rules

Views receive their information from the event rules that are enabled. Not all rules provided by the SFW Management Pack are enabled by default.

To enable or disable a rule, you must override the rule's current setting and save its changed state in another management pack. Changes are saved in the Default Management Pack by default, however you can isolate SFW rule changes in a custom pack set up exclusively for SFW rule changes.

For example, to enable MPIO path performance counters, you would do the following:

1. In the Authoring pane of the Operator Console, select the Rules object under Management Pack Objects to display the Rules pane.
2. Right-click the "Get MPIO Path Performance Data" rule in the Rules pane and select Overrides>Override the Rule.

   Note: The "Get MPIO Path Performance Data" rule can be found in the group, "Veritas Storage Foundation for Windows by Symantec Servers with DMP DSM Option Installation". The rule only applies to a SFW server that has the DMP DSM option installed, so right-click the "Get MPIO Path Performance Data" rule under "Veritas Storage Foundation for Windows by Symantec Servers with DMP DSM Option Installation".

3. In the context menu for Override the Rule, select "For all objects of type: Veritas Storage Foundation for Windows by Symantec Servers with DMP DSM Option Installation".
   The Override Properties window appears.
4. In the Override Properties window, check the Override checkbox and set the Override Setting pulldown value to True.
5. Set the destination management pack that will store the override settings for the SFW Management Pack.
   You can create one specifically for SFW by clicking **New** in the bottom right corner of the Override Properties window and working with the Create a Management Pack wizard that appears.
6. After setting up the destination management pack, click **Apply** to set the override setting for the rule's Enabled field to True.

   Note: Note that the rule's icon does not change after changing the setting. You can check a rule's current settings by right-clicking a rule and selecting Overrides Summary.

Monitoring SFW servers using views

The views supported by the SFW Management Pack are available through the Monitoring pane of the Operator Console. These views enable you to assess the state of the required SFW servers within the managed environment. The Monitoring pane supports the following views:

- Alert
- State
- Event
- Diagram
- Performance

Alert

Alert 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

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

SFW State

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

- **State for all SFW 4.3, and 5.x Servers**
  Displays the state for all the servers in the Veritas Storage Foundation Servers Computer Group.
- **State for Servers with DMP DSM Option**
  Displays the state for all the servers in the Veritas Storage Foundation 5.1 for Windows by Symantec Servers with DMP DSM Option Computer Group.

VVR State

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

The Veritas Volume Replicator event rules use scripts to collect the required VVR performance data or objects data. The VVR scripts are enabled by default

and fetch the VVR information from the servers. The VVR scripts require that the `vxvm` service be running on all the SFW servers. The following scripts are used by the VVR state:

- `VVR Objects Discovery Data`—Collects the VVR objects information and provides this information to the Opr Mgr 2007 server. By default, this script collects data every 15 minutes.
- `VVR Object State Monitoring Data`—Collects the VVR objects and state monitoring information and provides this information to the Opr Mgr server. By default, this script collects data every 9 minutes.

In the event that you need to disable the VVR scripts, you need to

1. Locate the following two timed events in the Ops Mgr 2007 server Authoring pane
   - VVR Objects State Monitoring
   - VVR Objects Discovery
2. Override the rule using steps described earlier, in the group "Veritas Storage Foundation for Windows by Symantec Servers with VVR Option Installation".

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 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 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
	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

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

Performance

Performance displays the tabulated information of SFW and VVR counters. You can select the required counters and click **Draw Graph** for the graphical

representation of the selected performance counters. Performance displays performance data only for DMP and VVR.

DMP DSM performance data counters

An event rule called “Get MPIO Performance Data” has been added to the Dynamic Multi-pathing\Veritas DMP DSMs (MPIO Device Specific Modules) rule category for the SFW Management Pack. This event rule and its data provider is a timed response which triggers an event every 15 minutes. This event rule is disabled by default.

When enabled, the event rule executes a vbscript on the Opr Mgr 2007 server. The vbscript executes `vxdmpadm.exe` on the SFW agent-managed computers where the DMP DSM option is installed. It uses the 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 Opr Mgr server with counter names in the format `counter name\path\device`. The counters are automatically added to the Opr Mgr 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. The event rules for DMP DSM performance are in “DMP DSM Path Performance Rules” on page 52.

Dynamic Disk, Dynamic Volume, and VVR performance data counters

Event rules for performance data for dynamic disks, dynamic volumes, and VVR are available in the SFW Management Pack. When enabled, these rules trigger an event every 15 minutes and returns performance data. These event rules are disabled by default and must be enabled for use. These event rules are described in “Disks, Disk Groups, and Volumes Performance Rules” on page 40 and in “Volume Replicator (VVR) Performance Rules” on page 73.

Chapter 4

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.

SFW Monitoring 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 4-1 lists the Disks, Disk Groups, and Volumes rules included in the SFW Management Pack.

Table 4-1 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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
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

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
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
775	VxSvc_vxvm	Split dynamic disk group failed.	Error	Yes	No
776	VxSvc_vxvm	Join dynamic disk group succeeded.	Success	No	No
777	VxSvc_vxvm	Join dynamic disk group failed.	Error	Yes	No
790	VxSvc_vxvm	Resynchronize volume succeeded.	Success	No	No
791	VxSvc_vxvm	Resynchronize volume failed.	Error	Yes	No
792	VxSvc_vxvm	Adding mirror succeeded.	Success	No	No
793	VxSvc_vxvm	Adding mirror failed.	Error	Yes	No
794	VxSvc_vxvm	Moving subdisk succeeded.	Success	No	No
795	VxSvc_vxvm	Moving subdisk failed.	Error	Yes	No
798	VxSvc_vxvm	Attaching mirror succeeded.	Success	No	No
799	VxSvc_vxvm	Attaching mirror failed.	Error	Yes	No
800	VxSvc_vxvm	Recover dynamic disk group succeeded.	Success	No	No

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
801	VxSvc_vxvm	Recover dynamic disk group failed.	Error	Yes	No
808	VxSvc_vxvm	SCSI reservation thread start failure.	Error	Yes	Yes
809	VxSvc_vxvm	SCSI Reservation Thread Stop Failure.	Error	Yes	Yes
810	VxSvc_vxvm	Private group registry entry failure.	Error	Yes	No
811	VxSvc_vxvm	SCSI reservation thread update failure.	Error	Yes	Yes
813	VxSvc_vxvm	Rename dynamic disk group succeeded.	Success	No	No
814	VxSvc_vxvm	Rename dynamic disk group failed.	Error	Yes	No
815	VxSvc_vxvm	Destroy dynamic disk group succeeded.	Success	No	No
816	VxSvc_vxvm	Destroy dynamic disk group failed.	Error	Yes	No
819	VxSvc_vxvm	Snap Back using snapshot succeeded.	Success	No	No
820	VxSvc_vxvm	Snap Back using snapshot failed.	Error	Yes	No
825	VxSvc_vxvm	Shrink volume succeeded	Warning	Yes	No
8087	VxSvc_vxvm	Hot Relocation/Spare succeeded.	Success	No	No
8088	VxSvc_vxvm	Hot Relocation/Spare failed.	Error	Yes	No
8089	VxSvc_vxvm	Unrelocate disk succeeded.	Success	No	No
8090	VxSvc_vxvm	Unrelocate disk failed.	Error	Yes	No

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
8091	VxSvc_vxvm	Remove disk from dynamic disk group succeeded.	Success	No	No
8092	VxSvc_vxvm	Remove disk from dynamic disk group failed.	Error	Yes	No
8093	VxSvc_vxvm	Reactivate disk succeeded.	Success	No	No
8094	VxSvc_vxvm	Reactivate disk failed.	Error	Yes	No
8095	VxSvc_vxvm	Evacuate disk succeeded.	Success	No	No
8096	VxSvc_vxvm	Evacuate disk failed.	Error	Yes	No
8097	VxSvc_vxvm	Add disk to dynamic disk group succeeded.	Success	No	No
8098	VxSvc_vxvm	Add disk to dynamic disk group failed.	Error	Yes	No
8099	VxSvc_vxvm	Replace disk succeeded.	Success	No	No
9000	VxSvc_vxvm	Replace disk failed.	Error	Yes	No
9001	VxSvc_vxvm	Merge foreign disk succeeded.	Success	No	No
9002	VxSvc_vxvm	Merge foreign disk failed.	Error	Yes	No
9003	VxSvc_vxvm	Move subdisk succeeded.	Information	No	No
9004	VxSvc_vxvm	Move subdisk failed.	Error	Yes	No
10001	VxSvc_vxvm	Physical disk was removed or is temporarily unavailable.	Warning	Yes	No
10006	VxSvc_vxvm	Force import dynamic disk group succeeded.	Information	No	No
10101	VxSvc_vxvm	Force import dynamic disk group failed.	Error	Yes	No
10106	VxSvc_vxvm	Force deport dynamic disk group succeeded.	Information	No	No

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
10111	VxSvc_vxvm	Force deport dynamic disk group failed.	Error	Yes	No
10120	VxSvc_vxvm	Automatic BOOT.INI update succeeded.	Information	Yes	Yes
10125	VxSvc_vxvm	Automatic BOOT.INI update failed.	Error	Yes	Yes
10131	VxSvc_vxvm	BOOT.INI update required.	Information	Yes	Yes
10201	VxSvc_vxvm	Mirror resynchronization started.	Information	No	No
10211	VxSvc_vxvm	Mirror resynchronization in progress.	Information	No	No
10221	VxSvc_vxvm	Mirror resynchronization completed.	Success	No	No
10226	VxSvc_vxvm	Import cluster dynamic disk group succeeded.	Success	No	No
10229	VxSvc_vxvm	Import cluster dynamic disk group failed.	Error	Yes	Yes
10232	VxSvc_vxvm	Deport cluster dynamic disk group succeeded.	Success	No	No
10235	VxSvc_vxvm	Deport cluster dynamic disk group failed.	Error	Yes	Yes
10238	VxSvc_vxvm	Cluster dynamic disk group deported with active I/O.	Warning	Yes	Yes
10242	VxSvc_vxvm	Could not lock all volumes. Cluster disk group was not deported.	Error	Yes	Yes
10251	VxSvc_vxvm	Mirror resynchronization failed.	Error	Yes	No
10256	VxSvc_vxvm	Dynamic disk group deported with active I/O.	Warning	Yes	No

Table 4-1 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
10260	VxSvc_vxvm	Could not lock all volumes. Dynamic disk group was not deported.	Error	Yes	No
10264	VxSvc_vxvm	Dynamic disk group failed.	Error	Yes	Yes
10268	Vxsvc_vxvm	Attach disk succeeded.	Information	No	No
10272	VxSvc_vxvm	Attach disk failed.	Error	Yes	Yes
10276	Vxsvc_vxvm	Detach disk succeeded.	Information	No	No
10280	VxSvc_vxvm	Detach disk failed.	Error	Yes	Yes
10284	Vxsvc_vxvm	vxcbr backup failed.	Error	Yes	Yes
10289	Vxsvc_vxvm	Shred volume succeeded.	Information	Yes	No
10293	Vxsvc_vxvm	Shred volume failed.	Error	Yes	Yes
10297	Vxsvc_vxvm	Shred volume started.	Information	Yes	No
10301	Vxsvc_vxvm	vxcbr manual backup failed.	Error	Yes	Yes
10306	Vxsvc_vxvm	Manually backup the dynamic disk group configuration.	Information	Yes	No

Disks, Disk Groups, and Volumes Performance Rules

Note: On 64-bit AMD64 and 64-bit Intel Xeon servers running the Microsoft Windows-on-Windows 64-bit (WOW64) subsystem, the SFW performance counters for dynamic disks and volumes cannot be viewed with the MOM 2005 Operator Console.

Table 4-2 Performance Rules

Rule Category	Rule Name	Provider	Sample Every	Rule Enabled
DDGV	Avg Time (microsecond)/Read Block	Dynamic Disk	15 minutes	No
DDGV	Avg Time(microsecond)/Write Block	Dynamic Disk	15 minutes	No
DDGV	Current Disk Queue Length	Dynamic Disk	15 minutes	No
DDGV	Read Block/sec	Dynamic Disk	15 minutes	No
DDGV	Read Request/sec	Dynamic Disk	15 minutes	No
DDGV	Write Block/sec	Dynamic Disk	15 minutes	No
DDGV	Write Request/sec	Dynamic Disk	15 minutes	No
DDGV	Avg Time(microsecond)/Read Block	Dynamic Volume	15 minutes	No
DDGV	Avg Time(microsecond)/Write Block	Dynamic Volume	15 minutes	No
DDGV	Read Block/sec	Dynamic Volume	15 minutes	No
DDGV	Read Request/sec	Dynamic Volume	15 minutes	No
DDGV	Write Block/sec	Dynamic Volume	15 minutes	No

Table 4-2 Performance Rules

Rule Category	Rule Name	Provider	Sample Every	Rule Enabled
DDGV	Write Request/sec	Dynamic Volume	15 minutes	No

Dynamic Multi-pathing Monitoring Rules

Dynamic Multi-pathing rules are located in the Veritas Storage Foundation for Windows folder. The following lists the Dynamic Multi-pathing rules for DMP Array Support Libraries (ASLs) and DMP Device Specific Modules (DSMs) included in the SFW Management Pack.

DMP Array Support Libraries (ASLs)

Table 4-3 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
3	VxDMP	Failed to initialize array specific information for this array.	Error	Yes	Yes
4	VxDMP	Failed to create DMP device object or disk filter device object.	Error	Yes	No
5	VxDMP	Failed to create symbolic link to device.	Error	Yes	No
6	VxDMP	Failure in IOCTL command.	Error	Yes	No
8	VxDMP	Failed to attach to path.	Information	No	No
9	VxDMP	Failed to allocate memory at the specified location within DMP.	Error	Yes	No
10	VxDMP	Failed to create path, device, or array object.	Error	Yes	Yes
11	VxDMP	Failure waiting for object.	Error	Yes	No

Table 4-3 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
12	VxDMP	Invalid partition information for device.	Error	Yes	No
13	VxDMP	DMP driver version mismatch for device.	Error	Yes	No
14	VxDMP	Cannot create NT directory object.	Error	Yes	No
15	VxDMP	Cannot create NT thread.	Error	Yes	No
16	VxDMP	Function table creation error.	Error	Yes	No
17	VxDMP	Cannot create notification event for user and kernel communication.	Error	Yes	No
18	VxDMP	Cannot read parameter value.	Information	No	No
19	VxDMP	Check sum error in parameter value.	Error	Yes	No
22	VxDMP	DMP cannot start this device properly. Detaching from device.	Error	Yes	No
23	VxDMP	Failed to open registry key.	Error	Yes	No
24	VxDMP	Failed to create registry key.	Error	Yes	No
25	VxDMP	Failed to close registry key.	Error	Yes	No
26	VxDMP	Failed to read registry key.	Error	Yes	No
27	VxDMP	Invalid parameter passed in function.	Error	Yes	No

Table 4-3 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
28	VxDMP	Buffer passed is smaller than the amount of data to be copied.	Error	Yes	No
31	VxDMP	SCSI miniport was excluded from DMP in AddDevice.	Information	No	No
32	VxDMP	Block I/O failed on harddisk.	Information	No	No
33	VxDMP	IRP failing with error status after VxDMP has attempted to send it through all connected paths.	Error	Yes	No
0	VxSvc_dmpprov	Path failed.	Error	Yes	No
1005	VxSvc_dmpprov	Set array monitor interval time succeeded.	Success	No	No
1010	VxSvc_dmpprov	Failed to set the array monitor interval time.	Error	Yes	No
1015	VxSvc_dmpprov	Enable path succeeded.	Success	No	No
1020	VxSvc_dmpprov	Enable path failed.	Error	Yes	No
1025	VxSvc_dmpprov	Disable path succeeded.	Success	No	No
1030	VxSvc_dmpprov	Disable path failed.	Error	Yes	No
1035	VxSvc_dmpprov	Successfully set mode to Active/Active.	Success	No	No
1040	VxSvc_dmpprov	Failed to set mode to Active/Active.	Error	Yes	No
1045	VxSvc_dmpprov	Successfully set mode to Active/Passive.	Success	No	No
1050	VxSvc_dmpprov	Failed to set the disk to Active/Passive mode.	Information	No	No
1055	VxSvc_dmpprov	Device exclude succeeded.	Success	No	No

Table 4-3 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
1060	VxSvc_dmpprov	Device exclude failed.	Error	Yes	No
1065	VxSvc_dmpprov	Device include succeeded.	Success	No	No
1070	VxSvc_dmpprov	Device include failed.	Error	Yes	No
1075	VxSvc_dmpprov	Array successfully set to Active/Active mode.	Success	No	No
1080	VxSvc_dmpprov	Failed to set the array to Active/Active mode.	Error	Yes	No
1085	VxSvc_dmpprov	Array successfully set to Active/Passive mode.	Success	No	No
1090	VxSvc_dmpprov	Failed to set the array to Active/Passive mode.	Error	Yes	No
1095	VxSvc_dmpprov	Array exclude succeeded.	Success	No	No
1100	VxSvc_dmpprov	Array exclude failed.	Error	Yes	No
1105	VxSvc_dmpprov	Array include succeeded.	Success	No	No
1110	VxSvc_dmpprov	Array include failed.	Error	Yes	No
1115	VxSvc_dmpprov	Successfully set preferred path.	Success	No	No
1120	VxSvc_dmpprov	Set preferred path failed.	Error	Yes	No
1125	VxSvc_dmpprov	Purge disks succeeded.	Information	No	No
1130	VxSvc_dmpprov	Purge disks failed.	Error	Yes	No
1135	VxSvc_dmpprov	Get tunable values succeeded.	Success	No	No
1140	VxSvc_dmpprov	Get tunable values failed.	Error	Yes	No
1145	VxSvc_dmpprov	Set tunable values succeeded.	Success	No	No

Table 4-3 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
1150	VxSvc_dmpprov	Set tunable values failed.	Error	Yes	No
1155	VxSvc_dmpprov	Failed path is now healthy.	Success	No	No

DMP Device Specific Modules (DSMs)

Note: In the table below, "MPIO DSM" in the Module column represents all the following:
- vemcclar (EMC CLARiiON arrays)
- vemcsymm (EMC DMX/Symmetrix arrays)
- vhdsap (HDS 95xx/WMS/AMS arrays)
- vhdsaa (HDS TagmaStore/99xx and HP XP arrays)
- vhpeva (HP EVA/MSA arrays)
- vibmaads (IBM DS8000/ESS800 arrays)
- vibmap (IBM DS6000 arrays)
- vengap (IBM DS4000 and Sun 6000 arrays)
- vnetapp (NetApp arrays)
- vitarget (Windows Storage Server 2003 R2 iSCSI arrays)
- vsparaa (3PARDATA arrays)
- vpillar (Pillar arrays)
- vibmapds (IBM DS AP arrays)

Table 4-4 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
1	MPIO DSM	MPIO Driver Specific Module (DSM) loaded.	Success	No	No
2	MPIO DSM	Failed to create DSM context.	Critical Error	Yes	Yes

Table 4-4 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
3	MPIO DSM	Failed to create array context.	Critical Error	Yes	Yes
4	MPIO DSM	Failed to create path context.	Critical Error	Yes	Yes
5	MPIO DSM	Failed to create device container context for SCSI ID.	Critical Error	Yes	Yes
6	MPIO DSM	Failed to register DSM with Microsoft Multipath I/O (MPIO).	Critical Error	Yes	Yes
7	MPIO DSM	Insufficient memory resources.	Critical Error	Yes	Yes
8	MPIO DSM	Failed to create device container. Maximum number of device containers exceeded.	Critical Error	Yes	Yes
9	MPIO DSM	Device explicitly excluded.	Information	No	No
10	MPIO DSM	Failed to perform path failover. Failing path not found.	Error	Yes	Yes
11	MPIO DSM	No path available to perform failover.	Critical Error	Yes	Yes
12	MPIO DSM	Device removed from array.	Warning	Yes	No
13	MPIO DSM	New device added to array.	Information	No	No
14	MPIO DSM	Path removed from array.	Warning	Yes	Yes
15	MPIO DSM	New path added to array.	Information	No	No
16	MPIO DSM	Cleared statistical information for all of array's devices.	Information	No	No

Table 4-4 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
17	MPIO DSM	Successfully changed load balance value for device(s) in array.	Information	No	No
18	MPIO DSM	Changed load balance value on all devices of array.	Information	No	No
19	MPIO DSM	Preferred path set for device(s) in array.	Information	No	No
20	MPIO DSM	Preferred path set for all devices in array.	Information	No	No
21	MPIO DSM	Changed array control parameters.	Information	No	No
22	MPIO DSM	Loaded global array control values.	Information	No	No
23	MPIO DSM	Loaded array control values.	Information	No	No
24	MPIO DSM	Loaded global load balance value.	Information	No	No
25	MPIO DSM	Loaded load balance value for array.	Information	No	No
26	MPIO DSM	Loaded group load balance value for device in array.	Information	No	No
27	MPIO DSM	Setting preferred path for array.	Information	No	No
28	MPIO DSM	Setting preferred path for group containing device in array.	Information	No	No
29	MPIO DSM	Failed to create registry key.	Error	Yes	No
30	MPIO DSM	Failed to create or replace registry value.	Error	Yes	No

Table 4-4 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
31	MPIO DSM	Failed to open registry key.	Error	Yes	No
32	MPIO DSM	Failed to close registry key.	Error	Yes	No
33	MPIO DSM	Failed to flush registry key.	Error	Yes	No
34	MPIO DSM	Failed to allocate memory for registry key.	Error	Yes	No
35	MPIO DSM	Found invalid value type in registry.	Error	Yes	No
36	MPIO DSM	Registry operation failed. Buffer too small.	Error	Yes	No
37	MPIO DSM	Registry value not found.	Error	Yes	No
38	MPIO DSM	Cannot create registry value.	Error	Yes	No
39	MPIO DSM	MPIO version mismatch.	Critical Error	Yes	Yes
40	MPIO DSM	Array product ID not supported by DSM.	Information	No	Yes
41	MPIO DSM	Special device type will not be claimed by DSM for array.	Information	No	No
42	MPIO DSM	Clear all statistical information for a device.	Information	No	No
43	MPIO DSM	Clear all statistical information for an array's devices.	Information	No	No
44	MPIO DSM	Enable SCSI-3 support in the registry for an array.	Information	No	No

Table 4-4 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
45	MPIO DSM	Disable SCSI-3 support in the registry for an array.	Information	No	No
46	MPIO DSM	No change of SCSI-3 support in the registry for an array.	Information	No	No
47	MPIO DSM	Ignore Scsi-3 support setting. The internal logic of DSM uses SCSI-3 for the array.	Information	No	No
48	MPIO DSM	Enable SCSI-3 support in the registry for a DSM.	Information	No	No
49	MPIO DSM	Disable SCSI-3 support in the registry for a DSM.	Information	No	No
50	MPIO DSM	Require action after setting SCSI-3 support.	Information	No	No
51	MPIO DSM	No change in the registry for SCSI-3 support setting of DSM.	Information	No	No
52	MPIO DSM	No change in the registry for SCSI-3 support setting with Next Generation Cluster.	Information	No	No
53	MPIO DSM	Ignore SCSI-3 support setting. The internal logic of DSM only uses SCSI-2 on the array.	Information	No	No
54	MPIO DSM	Successfully update Scsi-3 support for an array.	Information	No	No
55	MPIO DSM	Require action after setting SCSI-3 support.	Information	No	No

Table 4-4 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
56	MPIO DSM	Successfully update Scsi-3 support for a DSM.	Information	No	No
100	VxSvc_mpioprov	Path removed.	Warning	Yes	Yes
110	VxSvc_mpioprov	Path arrived.	Information	No	No
120	VxSvc_mpioprov	Array removed.	Warning	Yes	No
130	VxSvc_mpioprov	Array arrived.	Information	No	No
140	VxSvc_mpioprov	Successfully changed device load balance policy.	Success	No	No
150	VxSvc_mpioprov	Successfully set device primary path.	Success	No	No
160	VxSvc_mpioprov	Successfully changed array load balance policy.	Success	No	No
170	VxSvc_mpioprov	Successfully changed array primary path.	Success	No	No
180	VxSvc_mpioprov	Successfully changed array parameters.	Success	No	No
190	VxSvc_mpioprov	Successfully changed DSM load balance policy.	Success	No	No
200	VxSvc_mpioprov	Successfully changed DSM primary path.	Success	No	No
210	VxSvc_mpioprov	Successfully changed DSM parameters.	Success	No	No
220	VxSvc_mpioprov	Successfully reset device performance statistics.	Information	No	No
230	VxSvc_mpioprov	Successfully reset array performance statistics.	Information	No	No

Table 4-4 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
240	VxSvc_mpioprov	Successfully reset DSM performance statistics.	Information	No	No
250	VxSvc_mpioprov	Enable SCSI-3 support of DSM in the registry.	Information	No	No
254	VxSvc_mpioprov	Disable SCSI-3 support of DSM in the registry.	Information	No	No
260	VxSvc_mpioprov	Enable SCSI-3 support of an array in the registry.	Information	No	No
264	VxSvc_mpioprov	Disable SCSI-3 support of an array in the registry.	Information	No	No
270	VxSvc_mpioprov	No change of SCSI-3 support of an array.	Information	No	No
280	VxSvc_mpioprov	No change of SCSI-3 support status of DSM.	Information	No	No
290	VxSvc_mpioprov	Perform actions after SCSI-3 support setting.	Information	No	No
300	VxSvc_mpioprov	Change of SCSI-3 support is taking effect on the array.	Information	No	No
310	VxSvc_mpioprov	Next Generation Cluster support has been installed.	Information	No	No
320	VxSvc_mpioprov	SCSI-3 support status is always enabled.	Information	No	No
330	VxSvc_mpioprov	DSM uses SCSI-2 on the array only.	Information	No	No
340	VxSvc_mpioprov	Change of SCSI-3 is taking effect on DSM.	Information	No	No
350	VxSvc_mpioprov	The current status of SCSI-3 support on the array.	Information	No	No

Table 4-4 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
360	VxSvc_mpioprov	The current status of SCSI-3 support on DSM.	Information	No	No

DMP DSM Path Performance Rules

The following lists the DMP DSM path performance rules included in the SFW Management Pack. The Dynamic Multi-pathing\Veritas DMP DSMs (MPIO Device Specific Modules)\Get MPIO Performance Data rule must be enabled to generate this data. See "DMP DSM performance data counters" on page 24.

Table 4-5 DMP DSM Event Processing Rules

Rule Category	Rule Name	Provider	Sample Every	Rule Enabled
DMP DSMs	Number of Reads	DSM Path	15 minutes	No
DMP DSMs	Number of Writes	DSM Path	15 minutes	No
DMP DSMs	Bytes Read	DSM Path	15 minutes	No
DMP DSMs	Bytes Written	DSM Path	15 minutes	No

FlashSnap Monitoring Rules

FlashSnap rules are located in the Veritas Storage Foundation for Windows folder. The following lists the FlashSnap rules included in the SFW Management Pack.

Table 4-6 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
29	VxSvc_fastfileresync	Fast File Resync failed.	Error	Yes	No
31	VxSvc_fastfileresync	Fast File Resync completed successfully.	Success	No	No
1001	VxSvc_vssprov	Snapshot succeeded.	Success	No	No
1002	VxSvc_vssprov	Snapshot failed.	Error	Yes	No
1015	VxSvc_vssprov	Eseutil consistency check failed.	Error	Yes	No
1019	VxSvc_vssprov	Successfully refreshed VSS writers and components.	Success	No	No
1023	VxSvc_vssprov	Database restored successfully.	Success	No	No
1027	VxSvc_vssprov	Snap Back (reattach) database succeeded.	Success	No	No
1031	VxSvc_vssprov	Started Eseutil check on file.	Information	No	No
1035	VxSvc_vssprov	Successfully completed Eseutil check on file.	Success	No	No
1039	VxSvc_vssprov	Successfully Dismounted the database(s).	Information	No	No
1043	VxSvc_vssprov	Successfully Mounted the database(s).	Information	No	No
1047	VxSvc_vssprov	Failed to Dismount the database(s).	Information	No	No

Table 4-6 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
1051	VxSvc_vssprov	Failed to Mount the database(s).	Information	No	No
1064	VxSvc_vssprov	Synchronized snapshot validation failed.	Error	Yes	Yes
1068	VxSvc_vssprov	Synchronized snapback validation failed.	Error	Yes	Yes
1072	VxSvc_vssprov	VSS Writers refresh failure.	Information	No	No
1079	VxSvc_vssprov	Log Replay failed.	Error	Yes	Yes
1083	VxSvc_vssprov	Started Replaying log file.	Information	No	No
1087	VxSvc_vssprov	Successfully replayed log file.	Information	No	No
1092	VxSvc_vssprov	Database(s) restored successfully to recovery storage group.	Success	No	No
1096	VxSvc_vssprov	Database(s) restore to recovery storage group failed.	Error	Yes	No

Licensing Monitoring Rules

Licensing rules are located in the Veritas Storage Foundation for Windows folder. The following lists the Licensing rules included in the SFW Management Pack.

Table 4-7 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
7000	VxSvc_sysprov	Duplicate license detected.	Warning	Yes	Yes
7004	VxSvc_sysprov	Evaluation license will expire shortly.	Warning	Yes	Yes
7008	VxSvc_sysprov	Evaluation license expired.	Warning	Yes	Yes
7012	VxSvc_sysprov	Product license is invalid.	Warning	Yes	Yes
7016	VxSvc_sysprov	License authorized usage exceeded.	Warning	Yes	Yes

VxCache Monitoring Rules

VxCache rules are located in the Veritas Storage Foundation for Windows folder. The following lists the VxCache rules included in the SFW Management Pack.

Table 4-8 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
2	vxcache	Cache configured successfully.	Information	No	No
3	vxcache	Cache configuration failed.	Error	Yes	No
4	vxcache	Failed to enable caching for specified volume.	Error	Yes	No
5	vxcache	Caching enabled successfully for specified volume.	Information	No	No
6	vxcache	Successfully disabled caching on the specified volume.	Information	No	No
7	vxcache	Error disabling cache on object.	Error	Yes	No
11	vxcache	I/O between cache and disk failed.	Critical Error	Yes	Yes
12	vxcache	Failed to create filter device object.	Error	Yes	No
13	vxcache	Failure while attaching device to PDO.	Error	Yes	No
14	vxcache	Device IO offset error.	Warning	Yes	No
15	vxcache	Device IOCTL error.	Error	Yes	No
17	vxcache	Failure during alignment check.	Critical Error	Yes	Yes
18	vxcache	All I/O buffers in use, will retry.	Warning	Yes	No
19	vxcache	I/O failed between cache and disk.	Critical Error	Yes	Yes

Table 4-8 Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
21	vxcache	VxCache was not tested on this version of Windows.	Warning	Yes	No
22	vxcache	Failed to deallocate cache memory.	Error	Yes	No
1005	VxSvc_VxPolicyManager	Successfully enabled cache at server level.	Success	No	No
1010	VxSvc_VxPolicyManager	Enable cache at server level failed.	Error	Yes	No
1015	VxSvc_VxPolicyManager	Successfully disabled cache at server level.	Success	No	No
1020	VxSvc_VxPolicyManager	Disable cache at server level failed.	Error	Yes	No
1025	VxSvc_VxPolicyManager	Successfully enabled cache at volume level.	Success	No	No
1030	VxSvc_VxPolicyManager	Enable cache at volume level failed.	Error	Yes	No
1035	VxSvc_VxPolicyManager	Successfully disabled cache at volume level.	Success	No	No
1040	VxSvc_VxPolicyManager	Disable cache at volume level failed.	Error	Yes	No
1044	VxSvc_VxPolicyManager	Successfully reallocated cache memory at server level.	Success	No	No
1048	VxSvc_VxPolicyManager	Reallocation of cache memory at server level failed.	Error	Yes	No

Volume Replicator (VVR) Monitoring Rules

Volumes Replicator rules are located in the Veritas Storage Foundation for Windows folder. The following lists the Volumes Replicator rules included in the Management Pack.

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
80	vxio	Connection server started successfully.	Success	No	No
81	vxio	Failed to start connection server.	Critical Error	Yes	Yes
82	vxio	Connection server already started.	Information	No	No
83	vxio	TdiSendDatagramHB failed.	Error	Yes	No
84	vxio	NMCOM_send failed.	Error	Yes	No
85	vxio	Paused replay on RVG.	Information	No	No
86	vxio	Resumed replay on RVG.	Information	No	No
87	vxio	Latency throttling enabled for RLINK.	Information	No	No
88	vxio	Latency throttling disabled for RLINK.	Information	No	No
89	vxio	Latency throttling overridden on inactive RLINK.	Information	No	No
90	vxio	Latency throttling on inactive RLINK is causing I/O failures.	Information	No	No
91	vxio	Log overflow protection for RLINK triggered throttling.	Information	No	No
92	vxio	Log overflow protection throttling disabled for RLINK.	Information	No	No
93	vxio	Log overflow protection overridden on inactive RLINK.	Information	No	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
94	vxio	Log overflow protection on inactive RLINK is causing I/O failures.	Critical Error	Yes	Yes
95	vxio	Log overflow protection on inactive RLINK triggered DCM protection.	Information	No	Yes
96	vxio	DCM replay complete on RLINK.	Information	No	No
97	vxio	RLINK STALE (detached) due to log overflow.	Critical Error	Yes	Yes
98	vxio	RLINK connected to remote host.	Information	No	No
99	vxio	RLINK disconnected from remote host.	Information	No	No
100	vxio	Log capacity threshold reached for RLINK.	Information	No	No
101	vxio	Recovery started for RVG.	Information	No	No
102	vxio	RVG has been recovered successfully.	Success	No	Yes
103	vxio	Failed to recover RVG.	Critical Error	Yes	Yes
104	vxio	Detected Replicator Log volume failure while recovering RVG.	Critical Error	Yes	Yes
105	vxio	Detected configuration error while recovering RVG.	Critical Error	Yes	Yes
106	vxio	Inconsistent Replicator Log for RVG - detaching all Secondary nodes.	Critical Error	Yes	Yes
107	vxio	Replicator Log header version mismatch for RVG.	Critical Error	Yes	Yes
108	vxio	Failed to log the detach of the DCM volume.	Error	Yes	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
109	vxio	DCM volume is detached.	Error	Yes	No
110	vxio	Disconnecting Secondary due to ack timeout.	Error	Yes	No
111	vxio	Failed to activate DCM for RVG.	Error	Yes	No
112	vxio	Cannot recover volume.	Error	Yes	No
113	vxio	Received 100 duplicate packets.	Information	No	No
114	vxio	Disconnecting RLINK due to transaction deadlock.	Error	Yes	Yes
115	vxio	Invalid port range specified.	Critical Error	Yes	Yes
116	vxio	Cannot find any free port to bind.	Critical Error	Yes	Yes
117	vxio	Number of ports available is less than the number of RLINKs in the system.	Error	Yes	Yes
118	vxio	VVR data port range.	Information	No	No
119	vxio	Another application is using port. No free port is available within the specified range.	Error	Yes	Yes
120	vxio	Retry count exceeded the limit. Disconnecting RLINK.	Error	Yes	Yes
121	vxio	Packet size changed for RLINK.	Information	No	No
122	vxio	Invalid value ignored.	Information	No	No
123	vxio	Not enough resources to send updates over the network. Disconnecting RLINK.	Information	No	No
124	vxio	DCM logs are inaccessible to the volumes. DCM logging aborted.	Critical Error	Yes	Yes

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
125	vxio	I/O error on Replicator Log during recovery. Detaching the primary RLINK.	Critical Error	Yes	Yes
126	vxio	Primary RVG appears to have secondary Replicator Log.	Error	Yes	No
127	vxio	Secondary RVG appears to have primary Replicator Log.	Error	Yes	No
128	vxio	Failing writes on RVG. Remote host is now the primary RVG.	Information	No	No
129	vxio	Disconnecting RLINK to shift to DCM protection.	Information	No	No
130	vxio	Detaching RLINK due to I/O error on remote Replicator Log.	Critical Error	Yes	Yes
131	vxio	Incorrect magic number or unexpected upid (1) RVG.	Critical Error	Yes	Yes
132	vxio	Incorrect magic number or unexpected upid (2) RVG.	Critical Error	Yes	Yes
133	vxio	Invalid RVG update header.	Critical Error	Yes	Yes
134	vxio	Connection retry count exceeded 50. Disconnecting RLINK.	Error	Yes	No
135	vxio	RLINK is stale and not replicating.	Information	No	No
136	vxio	Secondary RLINK is paused.	Information	No	No
137	vxio	Primary RLINK is paused.	Information	No	No
138	vxio	RLINK is in failed state.	Information	No	No
139	vxio	RLINK is inconsistent.	Information	No	No
140	vxio	RLINK has a secondary log error.	Information	No	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
141	vxio	RLINK has a secondary config error.	Information	No	No
142	vxio	Failing writes on RVG. Remote is now a Primary RVG.	Information	No	No
143	vxio	Detaching RLINK due to I/O error on remote Replicator Log during recovery.	Critical Error	Yes	Yes
144	vxio	Volume has been removed from RVG and will no longer receive replication updates.	Information	No	No
145	vxio	Encountered IBC message while flushing Replicator Log to DCM - IBC dropped.	Information	No	No
146	vxio	Replicator Log for RVG contains earlier version of Replicator Log header.	Critical Error	Yes	Yes
147	vxio	Inconsistent update IDs.	Critical Error	Yes	Yes
148	vxio	Replication frozen for RLINK.	Information	No	No
149	vxio	IBC messages discarded for RLINK due to timeout.	Information	No	No
150	vxio	RLINK paused on secondary due to configuration error.	Information	No	Yes
151	vxio	Cannot connect to remote host due to header format mismatch or checksum error.	Critical Error	Yes	Yes
152	vxio	RVG unable to connect to RLINK.	Information	No	No
153	vxio	RLINK connection error.	Information	No	No
154	vxio	RLINK is in synchronous mode.	Information	No	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
155	vxio	RLINK is in asynchronous mode.	Information	No	No
156	vxio	Replication unfrozen for RLINK.	Information	No	No
157	vxio	RVG role is transitioning from primary to secondary.	Information	No	No
158	vxio	RVG role is transitioning from secondary to primary.	Information	No	No
159	vxio	RVG role is transitioning from primary to acting secondary.	Information	No	No
256	vxio	RVG role is transitioning from acting secondary to primary.	Information	No	No
257	vxio	RVG waiting for dismount request to complete.	Information	No	No
258	vxio	No volume with the specified tag was found in the RVG.	Critical Error	Yes	Yes
259	vxio	RVG state transition from acting secondary to secondary.	Information	No	No
260	vxio	RLINK switched from FAIL to ACTIVE due to secondary state change.	Information	No	No
261	vxio	Readback pool memory allocation failure for RVG.	Critical Error	Yes	Yes
262	vxio	NMCOM pool memory allocation failure for RVG.	Critical Error	Yes	Yes
263	vxio	Cannot spawn NMCOM_sender thread.	Critical Error	Yes	Yes
264	vxio	The resize operation failed to resize the Replicator Log volume. Replicator Log map is full.	Error	Yes	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
265	vxio	Replicator log map is coalesced. The Replicator Log can be resized a limited number of times.	Error	Yes	No
266	vxio	Cannot find Replicator Log Volume for RVG	Warning	Yes	No
267	vxio	Replicator Log Volume sizes on Primary and Bunker Secondary do not match	Error	Yes	Yes
267	vxio	VVR objects state monitoring	Critical Error	Yes	No
268	vxio	Cannot find valid start position for RVG	Error	Yes	No
269	vxio	Srl search sio returned error	Error	Yes	No
270	vxio	Flushing the logged srl writes for RVG	Information	No	No
271	vxio	Log flush failed for RVG during takeover	Error	Yes	No
287	vxio	Cannot connect RLINK due to protocol mismatch with remote RLINK	Error	Yes	Yes
303	vxio	RLINK disconnecting due to error	Error	Yes	No
319	vxio	RLINK encountered unknown error	Error	Yes	Yes
335	vxio	I/O error on storage bunker RLINK	Error	Yes	Yes
336	vxio	Disconnecting RLINK to complete DCM replay from SRL using internal checkpoint.	Information	No	No
337	vxio	Readback memory pool request failed for RLINK	Error	Yes	Yes

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
1286	vxio	VVR NPP Memory usage reduction factor has been set	Information	Yes	Yes
338	vxio	Versions of RVGs on local and remote host do not match	Warning	Yes	Yes
339	vxio	RVG replicator log config table is corrupted.	Warning	Yes	Yes
750	VxSvc_vvr	Primary RVG created.	Success	No	No
751	VxSvc_vvr	Failed to create RVG.	Error	Yes	No
756	VxSvc_vvr	Volume added to the RDS.	Success	No	No
757	VxSvc_vvr	Replicator Log volume added to the RVG.	Success	No	No
758	VxSvc_vvr	Data volume removed from the RDS.	Success	No	No
759	VxSvc_vvr	Replicator Log removed from RVG.	Success	No	No
760	VxSvc_vvr	RVG recovery completed.	Information	No	No
761	VxSvc_vvr	Failed to recover RVG.	Error	Yes	No
762	VxSvc_vvr	RVG checkstarted.	Success	No	No
763	VxSvc_vvr	Failed to checkstart RVG.	Error	Yes	No
764	VxSvc_vvr	Checkend on RVG successful.	Success	No	No
765	VxSvc_vvr	Failed to checkend RVG.	Error	Yes	No
766	VxSvc_vvr	Primary RVG deleted.	Success	No	No
767	VxSvc_vvr	Failed to delete RVG.	Error	Yes	No
776	VxSvc_vvr	Secondary paused.Replication to the secondary is paused.	Success	No	No
777	VxSvc_vvr	Failed to pause secondary.	Error	Yes	No
778	VxSvc_vvr	Secondary resumed.	Success	No	No
779	VxSvc_vvr	Failed to resume secondary.	Error	Yes	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
782	VxSvc_vvr	Secondary link recovered successfully.	Information	No	No
783	VxSvc_vvr	Failed to recover secondary link.	Error	Yes	No
784	VxSvc_vvr	Secondary restored successfully.	Success	No	No
785	VxSvc_vvr	Failed to restore secondary.	Error	Yes	No
786	VxSvc_vvr	Replicator Log failed.	Critical Error	Yes	Yes
787	VxSvc_vvr	Secondary disconnected.	Information	No	Yes
788	VxSvc_vvr	Volume under RVG failed.	Critical Error	Yes	Yes
789	VxSvc_vvr	Secondary connected.	Information	No	No
790	VxSvc_vvr	Secondary inconsistent.	Information	No	No
791	VxSvc_vvr	Replicator Log header error.	Critical Error	Yes	Yes
792	VxSvc_vvr	Replicator Log error on secondary.	Critical Error	Yes	Yes
793	VxSvc_vvr	Configuration error on secondary.	Critical Error	Yes	Yes
794	VxSvc_vvr	DCM logs are in use.	Information	No	No
795	VxSvc_vvr	Autosync is in progress.	Information	No	No
797	VxSvc_vvr	Secondary added. (Secondary host added to RDS).	Success	No	No
798	VxSvc_vvr	Change in replication mode.	Success	No	No
799	VxSvc_vvr	Change in latency protection.	Success	No	No
800	VxSvc_vvr	Change in Replicator Log protection.	Success	No	No
801	VxSvc_vvr	Change in latency high mark value.	Success	No	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
802	VxSvc_vvr	Change in latency low mark value.	Success	No	No
803	VxSvc_vvr	Change in packet size.	Success	No	No
805	VxSvc_vvr	RVG failed.	Critical Error	Yes	Yes
808	VxSvc_vvr	Secondary removed from RDS.	Success	No	No
809	VxSvc_vvr	RDS deleted.	Success	No	No
810	VxSvc_vvr	Failed to add secondary.	Error	Yes	No
811	VxSvc_vvr	Failed to delete the RDS.	Error	Yes	No
812	VxSvc_vvr	Failed to remove secondary.	Error	Yes	No
813	VxSvc_vvr	Failed to add volume.	Error	Yes	No
814	VxSvc_vvr	Failed to remove volume.	Error	Yes	No
815	VxSvc_vvr	Failed to resynchronize.	Error	Yes	No
816	VxSvc_vvr	Failed to add Replicator Log.	Error	Yes	No
817	VxSvc_vvr	Failed to remove Replicator Log.	Error	Yes	No
818	VxSvc_vvr	Resynchronization started.	Information	No	No
819	VxSvc_vvr	Resynchronization paused.	Information	No	Yes
820	VxSvc_vvr	Resynchronization resumed.	Information	No	No
821	VxSvc_vvr	Resynchronization completed.	Information	No	No
822	VxSvc_vvr	Secondary consistent.	Information	No	No
823	VxSvc_vvr	DCM activity completed.	Information	No	No
824	VxSvc_vvr	Autosync completed.	Information	No	No
825	VxSvc_vvr	Volume resize failed.	Error	Yes	No
832	VxSvc_vvr	Failed to convert RVG to primary.	Error	Yes	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
833	VxSvc_vvr	Failed to convert RVG to secondary.	Error	Yes	No
834	VxSvc_vvr	RVG is acting as secondary.	Information	No	No
835	VxSvc_vvr	RVG is converted to secondary.	Information	No	No
836	VxSvc_vvr	RVG is converted to primary.	Information	No	No
839	VxSvc_vvr	Acting secondary RVG deleted.	Success	No	No
842	VxSvc_vvr	Acting secondary paused.	Success	No	No
843	VxSvc_vvr	Failed to pause acting secondary.	Error	Yes	No
844	VxSvc_vvr	Acting secondary resumed.	Success	No	No
845	VxSvc_vvr	Failed to resume acting secondary.	Error	Yes	No
846	VxSvc_vvr	Acting Secondary link recovered.	Information	No	No
847	VxSvc_vvr	Failed to recover acting secondary link.	Error	Yes	No
848	VxSvc_vvr	Acting secondary connected.	Information	No	No
849	VxSvc_vvr	Acting secondary disconnected.	Information	No	Yes
850	VxSvc_vvr	Acting secondary inconsistent.	Information	No	No
851	VxSvc_vvr	Configuration error on acting secondary.	Critical Error	Yes	Yes
852	VxSvc_vvr	Replicator Log error on acting secondary.	Critical Error	Yes	Yes
853	VxSvc_vvr	Change in replication mode for acting secondary.	Success	No	No
854	VxSvc_vvr	Change in latency protection for acting secondary.	Success	No	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
855	VxSvc_vvr	Change in Replicator Log protection for acting secondary.	Success	No	No
856	VxSvc_vvr	Change in latency high mark value for acting secondary.	Success	No	No
857	VxSvc_vvr	Change in latency low mark value for acting secondary.	Success	No	No
858	VxSvc_vvr	Change in packet size for acting secondary.	Success	No	No
860	VxSvc_vvr	Acting secondary consistent.	Information	No	No
861	VxSvc_vvr	Failed to snapshot RVG.	Error	Yes	No
862	VxSvc_vvr	Failed to snapback RVG.	Error	Yes	No
864	VxSvc_vvr	Secondary ready to receive data.	Information	No	No
865	VxSvc_vvr	Replicator Log used.	Warning	Yes	Yes
866	VxSvc_vvr	Data access enabled for primary RVG.	Success	No	No
867	VxSvc_vvr	Failed to enable data access for RVG.	Error	Yes	No
868	VxSvc_vvr	Data access disabled for primary RVG.	Success	No	No
869	VxSvc_vvr	Failed to disable data access for RVG.	Error	Yes	No
870	VxSvc_vvr	Primary ready to send data to secondary.	Information	No	No
871	VxSvc_vvr	Failed to start replication on secondary.	Error	Yes	No
872	VxSvc_vvr	Replication stopped on secondary.	Success	No	No
873	VxSvc_vvr	Failed to stop replication on secondary.	Error	Yes	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
874	VxSvc_vvr	Data access enabled for secondary RVG.	Success	No	No
875	VxSvc_vvr	Data access disabled for secondary RVG.	Success	No	No
876	VxSvc_vvr	Data access enabled for acting secondary.	Success	No	No
877	VxSvc_vvr	Data access disabled for acting secondary.	Success	No	No
878	VxSvc_vvr	Replication stopped on acting secondary.	Success	No	No
879	VxSvc_vvr	Failed to stop replication to acting secondary.	Error	Yes	No
980	VxSvc_vvr	Primary RVG volumes appear as RAW.	Warning	Yes	No
5117	VxSvc_vvr	Change in Network transport protocol	Success	No	No
5120	VxSvc_vvr	Change in network transport protocol for acting secondary	Success	No	No
5123	VxSvc_vvr	Change in bandwidth limit value.	Success	No	No
5126	VxSvc_vvr	Change in bandwidth limit value for acting secondary	Success	No	No
5129	VxSvc_vvr	Bandwidth throttling disabled for secondary.	Success	No	No
5132	VxSvc_vvr	Bandwidth throttling disabled for acting secondary	Success	No	No
5135	VxSvc_vvr	Checkpoint delete successful on RVG.	Success	No	No
5136	VxSvc_vvr	Checkpoint delete failed on RVG.	Error	Yes	No
5139	VxSvc_vvr	Checkpoint delete successful on secondary link.	Success	No	No

Table 4-9 VVR Event Rules

Event ID	Module	Rule Name	Severity	Event Enabled	Alert Enabled
5140	VxSvc_vvr	Checkpoint delete failed on secondary link.	Error	Yes	No
5147	VxSvc_vvr	Bunker secondary deleted from RDS.	Information	No	No
5150	VxSvc_vvr	Failed to delete the bunker secondary.	Error	Yes	No
5153	VxSvc_vvr	Bunker secondary added.	Information	No	No
5156	VxSvc_vvr	Failed to add bunker secondary.	Error	Yes	No
5173	VxSvc_vvr	Compression is enabled on secondary	Information	Yes	Yes
5176	VxSvc_vvr	Compression is disabled on secondary	Information	Yes	Yes

Volume Replicator (VVR) Performance Rules

Note: On 64-bit AMD64 and 64-bit Intel Xeon servers running the Microsoft Windows-on-Windows 64-bit (WOW64) subsystem, the SFW performance counters for VVR Memory and VVR Remote Hosts cannot be viewed with the 32-bit MOM 2005 Operator Console.

Table 4-10 Performance Rules

Rule Category	Rule Name	Provider	Sample Every	Rule Enabled
VVR	Allocated NMCOM Pool (KBytes)	VVR Memory	15 minutes	No
VVR	Allocated READBACK Memory Pool (KBytes)	VVR Memory	15 minutes	No
VVR	Allocated VOLIO Memory Pool (KBytes)	VVR Memory	15 minutes	No
VVR	Data Transmitted (KBytes)	VVR Remote Hosts	15 minutes	No
VVR	DCM Usage(%)	VVR Remote Hosts	15 minutes	No
VVR	Used SRL(%)	VVR Remote Hosts	15 minutes	No