Symantec Storage Foundation™ Management Pack Guide for Microsoft System Center Operations Manager 2012

Windows

SFW Management Pack

Symantec Storage Foundation™ Management Pack Guide for Microsoft System Center Operations Manager 2012

Product version: 6.x, 7.x

Document version: Rev 1

Technical Support

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

Symantec's support offerings include the following:

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

For information about Symantec's support offerings, you can visit our website at the following URL:

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

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

Contacting Technical Support

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

www.symantec.com/business/support/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:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

About Symantec Connect

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

http://www.symantec.com/connect/storage-management

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Contents

About the SFW Management Pack

This chapter includes the following topics:

Overview

The Symantec Storage Foundation for Windows Management Pack for Microsoft System Center Operations Manager (SCOM) monitors theSFW and SFW HA servers and generates events and, when necessary, alerts for critical events. The SFW Management Pack helps you monitor the events generated by the SFW components (such as disks, disk groups, and volumes), Volume Replicator, and DMPW. The SFW Management Pack collects and displays error, warning, and informational event messages.

The SFW Management Pack also creates necessary alerts for critical events that require your attention.

This guide provides information about how to deploy and configure the SFW Management Pack in your SCOM environment. Symantec provides you with a .mp file to enable SCOM monitoring for SFW. The .mp file must be imported and installed into SCOM to enable monitoring.The guide also provides information about how you can monitor SFW for Windows using the different views in the SCOM console. The views supported by the SFW Management Pack enable you to monitor the health of the different components within the managed SCOM environment.

This guide is intended for the Microsoft System Center Operations Manager (SCOM) administrator. For specific information about Microsoft System Center Operations Manager (SCOM), refer to the Microsoft SCOM 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.

Symantec Storage Foundation for Windows monitoring

Using the Monitoring pane of the Microsoft System Center Operations Manager (SCOM) console, you can view the status of the SFW servers and learn about the events and alerts generated by the servers. The top-level view for the SFW Management Pack is called Symantec Storage Foundation for Windows. The three folders under the top-level view provide information about the alerts, events, and state of the SFW servers. For more information, See "Monitoring the SFW Management Pack" on page 16.

Depending on the rule that has been set for an event, an appropriate event or alert is generated when the event is received on the SCOM server.

Table 1-1 indicates the event severity categories for the SFW Management Pack:

Table 1-1 SFW Management Pack event severity categories

Event severity	Description
INFORMATION	Indicates an informational event.
WARNING	Indicates a potential problem or a low-priority issue that does not require any immediate action.
ERROR	Indicates errors that require your attention.

There are alert rule categories in the SFW Management Pack that are used for monitoring the specific components. Each of the categories consist of a set of events that are used to monitor the specific components.

Table 1-2 indicates the alert rule categories of the SFW Management Pack:

Table 1-2 SFW Management Pack alert rule categories

Alert rule category	Description
Licensing	Monitors license-related issues and failures.

Table 1-2 SFW Management Pack alert rule categories *(continued)*

Alert rule category	Description
Symantec Storage Foundation for Windows	Monitors the operational status of SFW and generates alerts when necessary.
Symantec Storage Foundation Volume Replicator	Monitors the operational status of Volume Replicator and generates alerts when necessary.
Symantec Dynamic Multi-Pathing for Windows	Monitors the operational status of arrays managed by DMPW Array Support Libraries (ASLs) and DMPW MPIO Device Specific Modules (DSMs) and generates alerts when necessary.
FlashSnap	Monitors the operational status of FlashSnap and generates alerts when necessary.

Note: 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. For more information, refer to Microsoft SCOM documentation.

SFW servers with CVM or fast failover

In case of an SFW configuration with Cluster Volume Manager (CVM) or fast failover, the GAB/LLT components are present on the SFW-installed nodes. There is a new, separate Management Pack called "Symantec Cluster Communication Management Pack" that has GAB/LLT specific rules and alerts. To monitor events and alerts generated by the GAB/LLT components, you need to import this Management Pack separately. In the Monitoring pane, the events and alerts of this Management Pack are displayed under the global event and alert views and, if the SFW Management Pack is installed, under the SFW for Windows view as well.

For more information about the Symantec Cluster Communication Management Pack, refer to the *Symantec Storage Foundation and High Availability Cluster Communication Management Pack Guide for Microsoft SCOM*.

Deploying the SFW Management Pack

This chapter includes the following topics:

About deploying the SFW Management Pack

This chapter describes how to deploy and configure the SFW Management Pack in your existing Microsoft System Center Operations Manager (SCOM) environment.

Supported software

This section provides information about the supported software for the SFW Management Pack version 7.0.0.0.

Supported SCOM versions

- Microsoft System Center Operations Manager 2012 SP1
- Microsoft System Center Operations Manager 2012 R2

Supported product versions

- Symantec Storage Foundation for Windows 6.0

- Symantec Storage Foundation for Windows 6.0.1
- Symantec Storage Foundation for Windows 6.0.2
- Symantec Storage Foundation for Windows 6.1
- Symantec Storage Foundation and High Availability Solutions for Windows 6.0
- Symantec Storage Foundation and High Availability Solutions for Windows 6.0.1
- Symantec Storage Foundation and High Availability Solutions for Windows 6.0.2
- Symantec Storage Foundation and High Availability Solutions for Windows 6.1
- Veritas InfoScale Enterprise 7.0
- Veritas InfoScale Storage 7.0
- Veritas InfoScale Foundation 7.0

Prerequisites

Before deploying the SFW Management Pack, ensure that the following prerequisites are met:

- Ensure that the Microsoft System Center Operations Manager (SCOM) infrastructure is set up and running correctly. For more information, refer to the Microsoft SCOM documentation.

Moreover, if you want to monitor GAB/LLT components in an Symantec Storage Foundation configuration with Cluster Volume Manager (CVM) or fast failover, ensure that you install the Symantec Cluster Communication Management Pack that is available separately.

Deploying the SFW Management Pack

This section provides information about importing and installing the SFW Management Pack and about adding the SFW servers to SCOM for monitoring.

Importing the SFW Management Pack

The Symantec Storage Foundation for Windows Management Pack for Microsoft System Center Operations Manager (SCOM) is a sealed Management Pack named `Symantec.SFW.mp`. A sealed Management Pack means that you have the ability to make limited changes to the Management Pack. Perform the steps provided below to import and install the SFW Management Pack in SCOM.

To install the SFW Management Pack in SCOM:

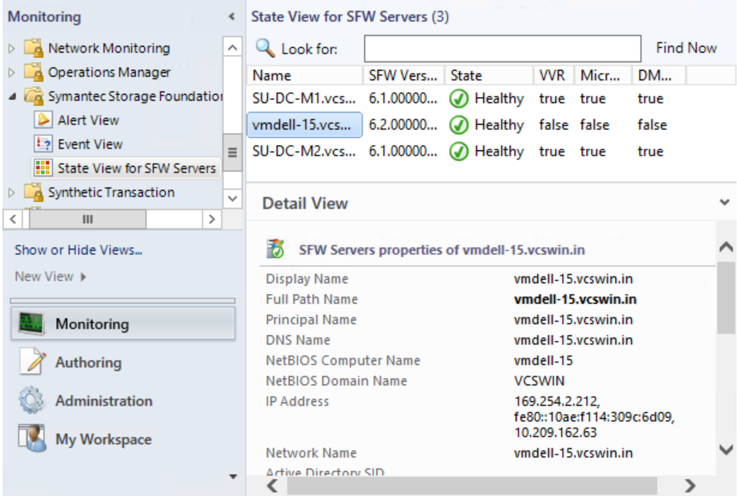
1. In the SCOM console, click **Administration**.
2. Right-click **Management Packs**, and then click **Import Management Packs**. The Import Management Packs wizard opens.
3. In the wizard, click **Add**, and then click **Add from disk**. The "Select Management Packs to import" dialog box appears.
4. In the dialog box, navigate to the SFW Management Pack file `Symantec.SFW.mp` and select it. The SFW Management Pack "Symantec SFW" with version 7.0.0.0 is listed.
5. Click **Install** to install the SFW Management Pack for SCOM.
6. Click **Close** to close the wizard.

When the Management Pack is successfully imported, it is listed under **Administration** > **Management Packs** in the SCOM console.

To view the SFW Management Pack alerts and events and the state of SFW servers, click **Monitoring** in the SCOM console and then select **Symantec Storage Foundation for Windows**.

Figure 2-1 shows the State view of Symantec Storage Foundation for Windows providing information about the current state of SFW servers.

Figure 2-1 State view of Symantec Storage Foundation for Windows



State View for SFW Servers (3)

Name	SFW Vers...	State	VVR	Micr...	DM...
SU-DC-M1.vcs...	6.1.00000...	✓ Healthy	true	true	true
vmdell-15.vcs...	6.2.00000...	✓ Healthy	false	false	false
SU-DC-M2.vcs...	6.1.00000...	✓ Healthy	true	true	true

SFW Servers properties of vmdell-15.vcswin.in

Display Name	vmdell-15.vcswin.in
Full Path Name	**vmdell-15.vcswin.in**
Principal Name	vmdell-15.vcswin.in
DNS Name	vmdell-15.vcswin.in
NetBIOS Computer Name	vmdell-15
NetBIOS Domain Name	VCSWIN
IP Address	169.254.2.212, fe80::10ae:f114:309c:6d09, 10.209.162.63
Network Name	vmdell-15.vcswin.in
Active Directory SID	

Adding SFW servers to SCOM for monitoring

This section provides information about adding SFW and SFW HA servers to Microsoft System Center Operations Manager (SCOM) for monitoring.

To monitor SFW servers for the SFW Management Pack, you need to add them to SCOM. Perform the steps provided below to discover and add SFW servers to SCOM for monitoring events and status of the servers.

Note: The following instructions are provided in brief. For detailed instructions and information, refer to the Microsoft SCOM documentation.

To add SFW servers to SCOM for monitoring:

1. In the Operations console, click **Administration**.
2. At the bottom of the navigation pane, click **Discovery Wizard**. This opens the Computer and Device Management Wizard.
3. On the Discovery Type panel, click **Windows computers**, and then click **Next**.
4. On the Auto or Advanced? panel, select appropriate options, and then click **Next**.
5. On the Discovery Method panel, select appropriate options and provide required information, and then click **Next**.
6. On the Administrator Account panel, select appropriate options and provide required information, and then click **Discover** to discover SFW servers.
7. On the Select Objects to Manage panel, after the discovery process is completed, the wizard lists all the discovered servers. Select the SFW servers that you want to add to SCOM for monitoring. Select Agent as the Management Mode.

   Click **Next**.
8. On the Summary panel, select appropriate options and provide required information, and then click **Finish**.
9. The Agent Management Task Status window opens. It shows the progress of adding SFW servers to SCOM.

   After the task completes, the added SFW servers are listed under **Administration** > **Device Management** > **Agent Managed** in the SCOM console.

Technical reference

This section provides information about targets and discovery objects that are used to gather SFW information for the SFW Management Pack for SCOM.

SFW server target

This target represents all the servers where SFW is installed. You can see the discovered objects for this target if you go to the discovered inventory and select this target class.

The target has different attributes providing information about the installed SFW version and the features installed on an SFW server (Volume Replicator, Microsoft Failover Clustering, and DMPW features).

SFW version discovery

Discovers servers with SFW installed. It will check for the "Version" value from the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\VxSvc\CurrentVersion\VolumeManager
```

For a list of supported product versions, See "Supported software" on page 11..

SFW features discovery

Discovers whether an SFW feature is installed by checking for the following respective registry keys:

For the Volume Replicator feature (for SFW and SFW HA version 6.x):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veritas\VPI

\{F834E070-8D71-4c4b-B688-06964B88F3E8}\SolutionOptions\vrts.soln.opt.vvr
```

For the Volume Replicator feature (for Veritas InfoScale products version 7.x):

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\ProductOption\VVR
```

For the Microsoft Failover Clustering feature:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veritas\VPI

\{F834E070-8D71-4c4b-B688-06964B88F3E8}\SolutionOptions\vrts.soln.opt.mscs
```

For the DMPW feature:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\VxSvc\CurrentVersion\Providers\mpioprov
```

Chapter 3

Monitoring the SFW Management Pack and managing rules

This chapter includes the following topics:

About monitoring the SFW Management Pack and managing rules

This chapter provides information about how you can monitor the Symantec Storage Foundation for Windows Management Pack using the available views in Microsoft System Center Operations Manager (SCOM). The chapter also provides information about SFW Management Pack monitors and how to locate, enable, and disable event and alert rules. Using the views supported by the SFW Management Pack, you can monitor the health of different components within the managed SCOM environment.

Monitoring the SFW Management Pack

The views supported by the SFW Management Pack are available through the Monitoring pane of the SCOM console. Using these views, you can see events and alerts and assess the state of the SFW servers within the managed SCOM environment.

The Monitoring pane supports the following views for the SFW Management Pack:

- Alert view
- Event view
- State view for SFW servers

Note: Some non-SFW events and alerts, such as .NET app monitoring and Apm Scripting, can appear in the event and alert views of Symantec Storage Foundation for Windows. This is because the SFW Management Pack views are targeted to a "Windows.Server.Computer" derived class. Therefore, any non-SFW event for an object for this derived or its base class would also appear in the SFW views. This is a SCOM behavior and not SFW Management Pack specific implementation.

Alert view

The alert view provides a list of issues that require action. It provides the current state of the alerts indicating whether an alert is newly-reported or resolved.

Event view

The event view provides a list of events that have occurred on the SFW servers. Each event has the event description, event ID, and the source of the event problem.

Note: The event view for SFW Management Pack provides information about all the events of the Warning and Error levels, but it does not collect and display the Information level events by default. To collect and display Information events, you need to manually enable rules using overrides for a particular event source. For information about how to enable rules using overrides, refer to Microsoft documentation.

State view for SFW servers

The state view for the SFW servers provides a real-time, consolidated look at the health of the SFW and SFW HA servers within the managed environment, highlighting the servers that require attention.

The SFW state displays information about all the servers where SFW 6.0 or higher is installed. To see details of a server (such as full path name, IP address), select it and the details will appear in the pane below.

For each server, the state view provides information about the SFW version, the current state of the server and the features installed on the server.

Table 3-1 provides information about the three states of an SFW server.

Table 3-1 SFW server states

State	Appearance	Description
Healthy	✓	Indicates that the server is running normally.
Critical	⊗	Indicates that there is a problem on the server.
Healthy	✓	Indicates that either the server is not running or there are connectivity issues.

The state view also provides information about whether the Symantec Storage Foundation Volume Replicator, Microsoft Failover Clustering, and Symantec Dynamic Multi-Pathing for Windows features are installed on a server. If a feature is installed on the server, the value is shown as "true"; otherwise the value is shown as "false".

SFW Management Pack monitors

The SFW Management Pack for SCOM has monitors for the following SFW services:

- Veritas Enterprise Administrator (VEA) service
- Veritas Scheduler service
- Veritas VSS Provider service
- Veritas Volume Replicator Security service
- Veritas Volume Replicator First Failure Data Capture service

Managing rules

This section provides information about how you can locate, enable, and disable event and alert rules in the SCOM console.

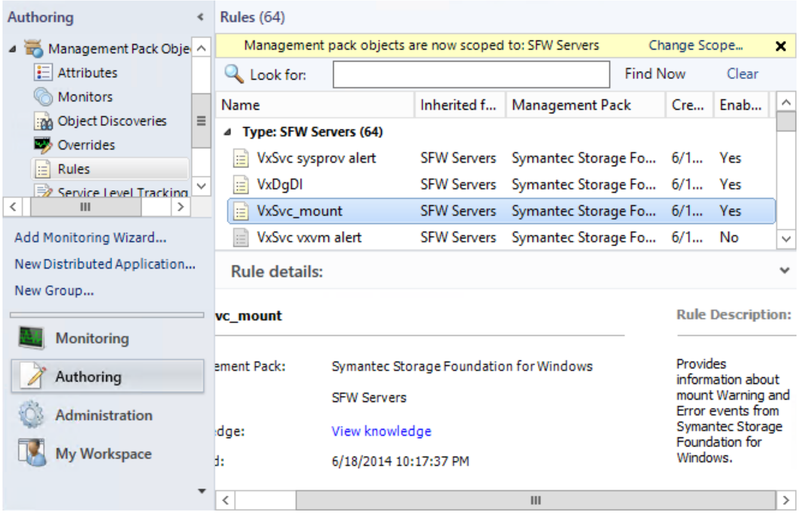
Locating rules

In the SCOM console, rules appear in a large list under the **Authoring** pane > **Management Pack Objects** > **Rules**.

You can narrow the scope of the rules being displayed (that is, filter the listed rules) by selecting **View** > **Scope** in the toolbar. In the Scope Management Pack Objects window that appears, you can select the SFW Servers as the target to display only the rules provided by the Symantec Storage Foundation for Windows Management Pack. You can easily search the SFW Servers target by entering "symantec" in the **Look for** search field.

Figure 3-1 shows the rules for the SFW Management Pack.

Figure 3-1 Symantec Storage Foundation Management Pack rules



Management pack objects are now scoped to: SFW Servers

Name	Inherited f...	Management Pack	Cre...	Enab...
Type: SFW Servers (64)				
VxSvc sysprov alert	SFW Servers	Symantec Storage Fo...	6/1...	Yes
VxDgDI	SFW Servers	Symantec Storage Fo...	6/1...	Yes
VxSvc_mount	SFW Servers	Symantec Storage Fo...	6/1...	Yes
VxSvc vxvm alert	SFW Servers	Symantec Storage Fo...	6/1...	No

vc_mount

ement Pack: Symantec Storage Foundation for Windows

SFW Servers

dge: View knowledge

d: 6/18/2014 10:17:37 PM

Rule Description:

Provides information about mount Warning and Error events from Symantec Storage Foundation for Windows.

To locate a rule, scroll through the list of rules or enter a search term in the **Look for** field at the top of the display. Using the **Look for** field, you can locate all instances of the rule regardless of the SFW group that contains it. For example, to locate rules with the word “alert” in their names, the search term "alert" can be used. Enter the search term in the **Look for** field and click **Find Now** to locate the rules and display the search results.

Enabling and disabling rules

Various views in the SCOM console receive information from the event rules that are enabled. However, 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 information about how to enable or disable rules using overrides, refer to Microsoft SCOM documentation.

Note: The event view for SFW Management Pack provides information about all the events of the Warning and Error levels, but it does not collect and display the Information level events by default. To collect and display Information events, you need to manually enable rules using overrides for a particular event source. For information about how to enable rules using overrides, refer to Microsoft SCOM documentation.

Event and alert rules

This chapter includes the following topics:

About rules

This chapter provides information about the event and alert rules for various SFW components for the SFW Management Pack for Microsoft System Center Operations Manager (SCOM). In the SFW Management Pack, the rules are used for generating events for analysis and reporting and, when necessary, raising alerts.

In the SCOM console, all the rules are for the SFW Management Pack target called "SFW Servers". Moreover, all the rules are displayed under the alert and event views under **Monitoring** > **Symantec Storage Foundation for Windows**.

Event rules

This section provides information about the event sources of the SFW components from which the SFW Management Pack generates events using rules. The events generated using the rules can be used for analysis and reporting.

Table 4-1 lists the Symantec Storage Foundation for Windows, Symantec Storage Foundation Volume Replicator, and Symantec Dynamic Multi-Pathing for Windows sources from which the SFW Management Pack generates events using rules.

Table 4-1 Event rule sources for SFW, Volume Replicator, and DMPW

Veritas Enterprise Administrator service	Vvrperf	VxSvc_fsys	VxSvc_sysprov
Veritas Scheduler Service	Vxboot	VxSvc_ftdisk	VxSvc_system
Veritas VDS Provider	VxDgDI	VxSvc_mount	VxSvc_vdsprov
Veritas VSS Provider	Vxio	VxSvc_mpioprov	VxSvc_vssprov
Vmperf	VxSvc_disk	VxSvc_pnp	VxSvc_vvr
VSS	VxSvc_dmpprov	VxSvc_scheduler	VxSvc_vxvm

Table 4-2 lists the DMPW MPIO Device Specific Module (DSM) sources from which the SFW Management Pack generates events using rules.

Table 4-2 Event rule sources for DMPW MPIO DSMs

v3paraa (3PARDATA)	vengap (IBM DS4000/SUN 6000)	vhpmsa2 (HP 2000)	vnexenta (NexentaStor)
vcomplnt (Compellent)	veqlogic (Dell EqualLogic)	vhuaweiap (HUAWEI S5300/S2300)	vnexsan (NEXSAN SATA/SAS Beast, E60/E18)
vdellmd (Dell MD3200, MD3200i)	vfujitsuaa (FUJITSU ETERNUS 2000)	vibmaads (IBM DS8000/ESS)	vpillar (PILLAR)
vemcclar (EMC Clarion)	vhdsaa (Hitachi TagmaStore/HP XP)	vibmap (IBM DS6000)	vsun (SUN)
vemcsymm (EMC Symmetrix/DMX)	vhdsap (Hitachi 95xx-AMS-WM)	vibmapds (IBM DS AP)	vviolin (VIOLIN V3000, V6000)
vemcvplx (EMC VPLEX)	vhpeva (HP EVA-MSA)	vnetapp (NETAPP)	vxiv (IBM XiV Storage System)

Alert rules

This section provides information about the event sources of the SFW components from which the SFW Management Pack generates alerts using rules. This section lists the alert rules for SFW, Volume Replicator, and DMPW.

Note: You can disable an alert rule using its alert rule name. For more information on how to disable an alert rule, refer to Microsoft SCOM documentation.

Licensing alert rules

Table 4-3 lists the licensing sources from which the SFW Management Pack generates alerts using rules.

Table 4-3 Alert rule sources for licensing

Event source	Event ID	Event message	Alert rule name	Alert enabled
VxSvc_sysprov	7000	Duplicate license detected.	VxSvc sysprov alert	Yes
VxSvc_sysprov	7004	Evaluation license will expire shortly.	VxSvc sysprov alert	Yes
VxSvc_sysprov	7008	Evaluation license expired.	VxSvc sysprov alert	Yes
VxSvc_sysprov	7012	Product license is invalid.	VxSvc sysprov alert	Yes
VxSvc_sysprov	7016	License authorized usage exceeded.	VxSvc sysprov alert	Yes
VxSvc_sysprov	7026	The product is no longer in licensing compliance even though it is still functioning properly.	VxSvc sysprov alert	Yes

SFW alert rules

Table 4-4 lists the Symantec Storage Foundation for Windows sources from which the SFW Management Pack generates alerts using rules.

Table 4-4 Alert rule sources for SFW

Event source	Event ID	Event message	Alert rule name	Alert enabled
Vxboot	Alerts will be generated for all events with severity Error and Warning.	Various messages.	Vxboot alert	Yes
Vxio	2	Failed to log DRL volume detach.	Vxio alert	Yes
Vxio	3	DRL volume is detached.	Vxio alert	Yes
Vxio	7	Kernel log full, object detached.	Vxio alert	Yes
Vxio	8	Kernel log update failed, object detached.	Vxio alert	Yes
Vxio	12	Double failure condition detected on RAID-5 volume.	Vxio alert	Yes
Vxio	13	Failure during RAID-5 logging operation.	Vxio alert	Yes
Vxio	29	Read error.	Vxio alert	Yes
Vxio	30	Write error.	Vxio alert	Yes
Vxio	41	Cluster or private disk group has lost access to a majority of its disks. Its reservation thread has been stopped.	Vxio alert	Yes
Vxio	50	Reservation thread stopped for cluster disk group. Cluster software may not be available.	Vxio alert	Yes
Vxio	52	Reservation refresh has been suspended.	Vxio alert	Yes
VxSvc_fsys	807	Volume capacity reached error condition.	VxSvc fsys alert	Yes

Table 4-4 Alert rule sources for SFW *(continued)*

Event source	Event ID	Event message	Alert rule name	Alert enabled
VxSvc_scheduler	807	Launch task failed.	VxSvc scheduler alert	Yes
VxSvc_vxvm	808	SCSI reservation thread start failure.	VxSvc vxvm alert	Yes
VxSvc_vxvm	809	SCSI Reservation Thread Stop Failure.	VxSvc vxvm alert	Yes
VxSvc_vxvm	811	SCSI reservation thread update failure.	VxSvc vxvm alert	Yes
VxSvc_vxvm	8088	Hot Relocation/Spare failed.	VxSvc vxvm alert	Yes
VxSvc_vxvm	10001	Physical disk was removed or is temporarily unavailable.	VxSvc vxvm alert	Yes
VxSvc_vxvm	10242	Could not lock all volumes. Cluster disk group was not deported.	VxSvc vxvm alert	Yes
VxSvc_vxvm	10260	Could not lock all volumes. Dynamic disk group was not deported.	VxSvc vxvm alert	Yes
VxSvc_vxvm	10284	vxcbr backup failed.	VxSvc vxvm alert	Yes
VxSvc_vxvm	10238	Cluster dynamic disk group deported with active I/O.	VxSvc vxvm alert	No
VxSvc_vxvm	10256	Dynamic disk group deported with active I/O.	VxSvc vxvm alert	No

Volume Replicator alert rules

Table 4-5 lists the Symantec Storage Foundation Volume Replicator sources from which the SFW Management Pack generates alerts using rules.

Table 4-5 Alert rule sources for Volume Replicator

Event source	Event ID	Event message	Alert rule name	Alert enabled
Vxio	81	Failed to start connection server.	Vxio alert	Yes
Vxio	90	Latency throttling on inactive RLINK is causing I/O failures.	Vxio alert	Yes
Vxio	91	Log overflow protection for RLINK triggered throttling.	Vxio alert	Yes
Vxio	94	Log overflow protection on inactive RLINK is causing I/O failures.	Vxio alert	Yes
Vxio	95	Log overflow protection on inactive RLINK triggered DCM protection.	Vxio alert	Yes
Vxio	97	RLINK STALE (detached) due to log overflow.	Vxio alert	Yes
Vxio	100	Log capacity threshold reached for RLINK.	Vxio alert	Yes
Vxio	103	Failed to recover RVG.	Vxio alert	Yes
Vxio	104	Detected Replicator Log volume failure while recovering RVG.	Vxio alert	Yes
Vxio	105	Detected configuration error while recovering RVG.	Vxio alert	Yes
Vxio	106	Inconsistent Replicator Log for RVG - detaching all Secondary nodes.	Vxio alert	Yes
Vxio	107	Replicator Log header version mismatch for RVG.	Vxio alert	Yes
Vxio	108	Failed to log the detach of the DCM volume.	Vxio alert	Yes
Vxio	109	DCM volume is detached.	Vxio alert	Yes
Vxio	111	Failed to activate DCM for RVG.	Vxio alert	Yes
Vxio	112	Cannot recover volume.	Vxio alert	Yes

Table 4-5 Alert rule sources for Volume Replicator *(continued)*

Event source	Event ID	Event message	Alert rule name	Alert enabled
Vxio	116	Cannot find any free port to bind.	Vxio alert	Yes
Vxio	124	DCM logs are inaccessible to the volumes. DCM logging aborted.	Vxio alert	Yes
Vxio	125	I/O error on Replicator Log during recovery. Detaching the primary RLINK.	Vxio alert	Yes
Vxio	126	Primary RVG appears to have secondary Replicator Log.	Vxio alert	Yes
Vxio	127	Secondary RVG appears to have primary Replicator Log.	Vxio alert	Yes
Vxio	130	Detaching RLINK due to I/O error on remote Replicator Log.	Vxio alert	Yes
Vxio	131	Incorrect magic number or unexpected upid (1) RVG.	Vxio alert	Yes
Vxio	132	Incorrect magic number or unexpected upid (2) RVG.	Vxio alert	Yes
Vxio	133	Invalid RVG update header.	Vxio alert	Yes
Vxio	140	RLINK has a secondary log error.	Vxio alert	Yes
Vxio	141	RLINK has a secondary config error.	Vxio alert	Yes
Vxio	143	Detaching RLINK due to I/O error on remote Replicator Log during recovery.	Vxio alert	Yes
Vxio	146	Replicator Log for RVG contains earlier version of Replicator Log header.	Vxio alert	Yes
Vxio	147	Inconsistent update IDs.	Vxio alert	Yes
Vxio	150	RLINK paused on secondary due to configuration error.	Vxio alert	Yes

Table 4-5 Alert rule sources for Volume Replicator *(continued)*

Event source	Event ID	Event message	Alert rule name	Alert enabled
Vxio	258	No volume with the specified tag was found in the RVG.	Vxio alert	Yes
Vxio	271	Log flush failed for RVG during takeover.	Vxio alert	Yes
Vxio	339	RVG replicator log config table is corrupted.	Vxio alert	Yes
VxSvc_vvr	786	Replicator Log failed.	VxSvc VVR alert	Yes
VxSvc_vvr	788	Volume under RVG failed.	VxSvc VVR alert	Yes
VxSvc_vvr	791	Replicator Log header error.	VxSvc VVR alert	Yes
VxSvc_vvr	792	Replicator Log error on secondary.	VxSvc VVR alert	Yes
VxSvc_vvr	793	Configuration error on secondary.	VxSvc VVR alert	Yes
VxSvc_vvr	805	RVG failed.	VxSvc VVR alert	Yes
VxSvc_vvr	851	Configuration error on acting secondary.	VxSvc VVR alert	Yes
VxSvc_vvr	852	Replicator Log error on acting secondary.	VxSvc VVR alert	Yes

DMPW alert rules

This section provides information about the Symantec Dynamic Multi-Pathing for Windows alert rules for DMPW Array Support Libraries (ASLs) and DMPW MPIO Device Specific Modules (DSMs) included in the SFW Management Pack.

Table 4-6 lists the DMPW MPIO DSM and DMPW ASL sources from which the SFW Management Pack generates alerts using rules.

Note: In the table below, "MPIO DSM" in the "Event source" column represents the MPIO DSMs listed in the "Event rules" section. For more information, See Table 4-2 on page 22.

Table 4-6 Alert rule sources for DMPW MPIO DSMs and DMPW ASLs

Event source	Event ID	Event message	Alert rule name	Alert enabled
MPIO DSM	3	Failed to create array context.	MPIO DSM alert	Yes
MPIO DSM	4	Failed to create path context.	MPIO DSM alert	Yes
MPIO DSM	5	Failed to create device container context for SCSI ID.	MPIO DSM alert	Yes
MPIO DSM	6	Failed to register DSM with Microsoft Multipath I/O (MPIO).	MPIO DSM alert	Yes
MPIO DSM	8	Failed to create device container. Maximum number of device containers exceeded.	MPIO DSM alert	Yes
MPIO DSM	10	Failed to perform path failover. Failing path not found.	MPIO DSM alert	Yes
MPIO DSM	11	No path available to perform failover.	MPIO DSM alert	Yes
MPIO DSM	12	Device removed from array.	MPIO DSM alert	Yes
MPIO DSM	14	Path removed fromarray.	MPIO DSM alert	Yes
MPIO DSM	39	MPIO version mismatch.	MPIO DSM alert	Yes
MPIO DSM	40	Array product ID not supported by DSM.	MPIO DSM alert	Yes
MPIO DSM	41	Special device type will not be claimed by DSM for array.	MPIO DSM alert	Yes
VxSvc_mpioprov	100	Path removed.	VxSvc mpioprov alert	Yes
VxSvc_mpioprov	120	Path arrived.	VxSvc mpioprov alert	Yes
VxSvc_dmpprov	0	Path failed.	VxSvc dmpprov alert	Yes

FlashSnap alert rules

Table 4-7 lists the FlashSnap sources from which the SFW Management Pack generates alerts using rules.

Table 4-7 Alert rule sources for FlashSnap

Event source	Event ID	Event message	Alert rule name	Alert enabled
VxSvc_vssprov	1064	Synchronized snapshot validation failed.	VxSvc vssprov alert	Yes
VxSvc_vssprov	1068	Synchronized snapback validation failed.	VxSvc vssprov alert	Yes
VxSvc_vssprov	1079	Log Replay failed.	VxSvc vssprov alert	Yes