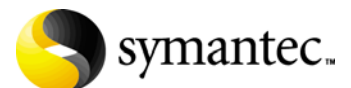


Veritas™ Cluster Server Management Pack Guide for Microsoft System Center Operations Manager 2007

Windows Server 2003,
Windows Server 2008

5.1

SQL Server 2008 support



Veritas Cluster Server Management Pack Guide for Microsoft System Center Operations Manager 2007

Copyright © 2009 Symantec Corporation. All rights reserved.

Veritas Cluster Server 5.1

Document Version: 5.1.1

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

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

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

The Licensed Software and Documentation are deemed to be “commercial computer software” and “commercial computer software documentation” as defined in FAR Sections 12.212 and DFARS Section 227.7202.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Third-party legal notices

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

Windows is a registered trademark of Microsoft Corporation.

Licensing and registration

Storage Foundation for Windows and Veritas Cluster Server are licensed products. See the *Storage Foundation and High Availability Solutions for Windows, Installation and Upgrade Guide* for license installation instructions.

Technical support

For technical assistance, visit <http://www.symantec.com/business/support/index.jsp> and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Chapter 1	VCS management pack overview	
	About VCS management packs	10
	Rules	12
	Alerts and Events	12
	Views	13
	Groups	14
Chapter 2	Deploying the VCS management packs	
	About deploying the VCS management packs	16
	Supported software	16
	Installing the Helper Process utility	17
	Importing the VCS management packs	18
	Importing the base VCS management pack	18
	Importing the VCS SQL or Exchange management pack	19
	Enabling VCS management pack monitoring	24
	Disabling additional monitoring for clustered instances	26
	Configuring cluster nodes	29
	Installing the Operations Manager 2007 agent	29
	Configuring agent-managed computers as proxy	31
	Adding physical servers to the group created	31
	Configuring clustered instances	33
	Adding clustered instances as agentless-managed objects	33
	Adding clustered instances to the empty Group	34
Chapter 3	Monitoring rules	
	About monitoring rules	36
	HAD monitoring rules	36
	GAB monitoring rules	65
	LLT monitoring rules	67
	Agents monitoring rules	68
	VMDg event processing rules	68
	MountV agent event processing rules	69
	ElifNone agent event processing rules	71
	FileNone agent event processing rules	71
	FileOnOff agent event processing rules	71

FileOnOnly agent event processing rules	72
FileShare agent event processing rules	72
Internet Information Services (IIS) agent event processing rules	73
GenericService event processing rules	77
Microsoft Virtual Machine (MSVirtualMachine) agent event processing rules	79
PrintShare agent event processing rules	80
PrintSpool agent event processing rules	81
Process agent event processing rules	83
Proxy agent event processing rules	85
IP agent event processing rules	85
IPMultiNicPlus agent event processing rules	86
NetLsnr agent event processing rules	89
NIC agent event processing rules	89
NotifierMgr agent event processing rules	90
Registry Replication (RegRep) agent event processing rules	91
Lanman agent event processing rules	93
VvrRvg agent event processing rules	96
RVGPrimary agent event processing rules	97
Enterprise application agents	101
MSDTC event processing rules	101
MSSearch event processing rules	103
SQL Server 2005 Agent Service event processing rules	104
SQL Server 2005 OLAP Service event processing rules	106
SQL Server 2005 event processing rules	107
SQL Sever 2000 event processing rules	109
Service Monitor event processing rules	112
Oracle Agent event processing rules	113
Exchange Service agent event processing rules	114
Exchange Protocol agent event processing rules	118
NetAppFiler agent event processing rules	121
NetAppSnapDrive agent event processing rules	122
NetAppSnapMirror agent event processing rules	122
Agent Framework monitoring rules	123

Appendix A Troubleshooting

About troubleshooting VCS management pack issues	138
Incorrect agent installation	138
Conflict while trying to monitor clusterized standalone instances	138
Error while re-importing the VCS management packs	139
Virtual computer discovery fails	140
Virtual computer fails to generate events or proxy computer is not set properly	

Additional discovery and monitoring of virtual computer for VCS	141
SQL Instances are not discovered on cluster nodes, where "Veritas High Availability engine" is not running	142
Index	143

VCS management pack overview

This chapter contains the following topics:

- [“About VCS management packs”](#) on page 10
- [“Rules”](#) on page 12
- [“Alerts and Events”](#) on page 12
- [“Views”](#) on page 13
- [“Groups”](#) on page 14

About VCS management packs

The Veritas Cluster Server (VCS) management packs for Operations Manager 2007 helps you monitor events generated by VCS components, as well as Microsoft SQL Server and Microsoft Exchange instances that are configured in a VCS cluster environment.

This guide provides information on the VCS management packs and instructions on how to import them in a Operations Manager 2007 monitoring environment.

The VCS management packs contain a set of rules that are based on the events placed in the Windows event log. These rules contain predefined alerts that are designed to notify you of critical events that require attention.

[Table 1-1](#) lists the VCS management packs for Operations Manager 2007.

Table 1-1 VCS management packs

File Name	Description
Symantec.SFW.HA.mp	Base VCS management pack that contains rules for monitoring VCS components.
Symantec.SQLServer.2000.mp	The VCS management pack for monitoring SQL Server 2000 instances.
Symantec.SQLServer.2005.mp	The VCS management pack for monitoring SQL Server 2005 instances.
Symantec.SQLServer.2008.mp	The VCS management pack for monitoring SQL Server 2008 instances.
Symantec.Exchange.Server.2003.mp	The VCS management pack for monitoring Exchange 2003 server.
Symantec.Exchange.Server.2007.mp	The VCS management pack for monitoring Exchange 2007 server.

You can find the VCS management packs in the following directory on the software DVD:

```
MOMPacks\cluster_server\storage_foundation_ha_for_windows\OP  
SMGR2007
```

The base VCS management pack, *Symantec.SFW.HA.mp*, is a sealed management pack that contains rules to monitor the following VCS components:

Table 1-2 Base VCS management pack: VCS components monitored

Component name	Description
Engine (HAD)	The high availability engine, or HAD, is the main VCS daemon running on each system. It is responsible for building the running cluster configuration from the configuration files, distributing the information when new nodes join the cluster, responding to operator input, and taking corrective action when something fails. The VCS Management Pack monitors the status of the HAD and notifies the user in case of errors.
GAB	Group Membership Services/Atomic Broadcast (GAB) is responsible for cluster membership and cluster communications. The VCS Management Pack monitors the status of the cluster memberships and communications.
LLT	VCS uses private network communications between cluster nodes for cluster maintenance. The Low Latency Transport (LLT) functions as a high-performance, low-latency replacement for the IP stack, and is used for all cluster communications. The VCS Management Pack monitors the LLT status.
Agents (Agent Framework)	The VCS Management Pack monitors the status of the VCS Bundled agents and Enterprise agents. The VCS agent framework is a set of common, predefined functions compiled into each agent. These functions include the ability to connect to the VCS engine (HAD) and to understand common configuration attributes. The agent framework frees the developer from developing support functions required by the cluster, and instead focus on controlling a specific resource type. The VCS management pack monitors the status of the common agent framework.

The base VCS management pack contains the following monitors:

- *VCS for Windows Installation by Symantec*
- *VeritasCluster*

These monitors are the targets for the rules defined in the base VCS management pack.

Rules

The base VCS management pack rules collect data, such as events, from the logs generated by the VCS components. Some of the rules have an associated alert that notifies the administrator about the event that triggered the alert.

You can view the VCS rules after you import the VCS management pack in Operations Manager 2007.

See [Chapter 3, “Monitoring rules”](#) on page 35 for a detailed list of VCS rules.

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 Operations Manager 2007 server. An alert notifies the administrator about the event that triggered the alert.

Each rule that generates the alert assigns an alert level that indicates the severity of that event. You can use the severity level to determine the importance of the alert and the necessary steps required to address the alert.

Note: The base VCS management pack does not include a notification group for automatic alerts by e-mail. If e-mail alerts are required, you must add the alert processing rules manually.

Views

Views are groups of managed objects that have a commonality, which is defined in the view properties. The views supported by the base VCS management pack enable you to monitor the health of the VCS components within the managed environment. These views enable you to assess the state of the required cluster node within the managed environment.

When you import the base VCS management pack, an item named *VCS for Windows by Symantec* is created under the Monitoring node in the Monitoring pane of the Operations Manager 2007 console. Expand **VCS for Windows by Symantec** to see the views supported by the base VCS management pack.

The following views are supported:

- **Active Alerts**

This view provides a list of alerts that are open and require action for computers in the *All Computers in Management Pack - Symantec.SFW.HA* group. It indicates the current state and severity of those alerts.

- **State View**

This view provides a real-time, consolidated look at the health of the cluster within the managed environment, highlighting the systems that require attention. It displays the state of the service groups and the resources configured in the service group.

In the Monitoring pane, expand **VCS for Windows by Symantec** and click **State View**. In the State View pane, click an item in the **VeritasCluster** column. The Detail View section displays the status of the service group and the resources. Depending on the state the status is displayed as follows:

- **Healthy:** Indicates that the service group and its resources are online on the node.
- **Warning:** Indicates that the service group is partially online on the node.
- **Critical:** Indicates that either the service group or the resources in the service group have faulted on the node.

Whenever a service group or a resource in a service group faults on a node, an appropriate alert is generated.

VCS management pack has a separate monitor for monitoring the health of the Veritas High Availability Daemon (HAD). If HAD is not running on a node, then an appropriate alert is generated. This alert stays active until the time HAD starts on that node. As soon as HAD starts on the node, this alert gets resolved automatically.

To enable the state view display for VCS, the following rules have been created in VCS for Windows Installation by Symantec:

- VeritasCluster Service Discovery
- VeritasCluster State Monitoring

The scripts that these rules invoke, internally use the `MOMUtil.exe` utility. The `MOMUtil` utility discovers all the service groups and resources in the cluster and then gathers the state related information for all the service groups and resources.

- Alerts
Displays alerts for the VCS components: Agents, Engine, GAB, and LLT. This view provides a list of issues 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.
- Events
Displays events for the VCS components: Agents, Engine, GAB, and LLT. The Event view provides a list of events that have occurred on managed servers, a description of each event, and the source of the problem.

Groups

Groups in Operations Manager 2007 are logical collections of objects such as computers, hard-disks, or instances of SQL or Exchange. Groups help define on which computers the rules are deployed. When you import the base VCS management pack, the following groups are created:

- VCS for Windows by Symantec Computer Group—Includes Windows servers running Veritas Cluster Server 5.1 or later.
- All Computers in ManagementPack: Symantec.SFW.HA—Contains all the computers that are discovered as a part of other computer groups defined in ManagementPack Symantec.SFW.HA

These groups are located under the Groups node in the Authoring pane of the Operations Manager 2007 Console.

Deploying the VCS management packs

This chapter contains the following topics:

- [“About deploying the VCS management packs”](#) on page 16
- [“Supported software”](#) on page 16
- [“Installing the Helper Process utility”](#) on page 17
- [“Importing the VCS management packs”](#) on page 18
- [“Enabling VCS management pack monitoring”](#) on page 24
- [“Configuring cluster nodes”](#) on page 29
- [“Configuring cluster nodes”](#) on page 29

About deploying the VCS management packs

This chapter describes how to deploy the VCS management packs in a Microsoft Systems Center Operations Manager 2007 monitoring environment. Complete the procedures in the given order.

Supported software

The VCS management packs are compatible with:

- Microsoft System Center Operations Manager 2007 SP1
- Veritas Cluster Server 5.1 for Windows
- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007

Installing the Helper Process utility

This procedure is required only if you plan to import the VCS SQL or Exchange management pack for Operations Manager 2007.

In Operations Manager 2007, managed items are collectively referred to as objects. Computers can be either be agent managed or agentless managed objects. Each agentless managed computer must be associated with an agent-managed computer (physical system) that acts as a proxy and provides remote agent functionality for the virtual server. Operations Manager 2007 server retrieves agentless managed object related events from its associated agent-managed proxy.

SQL or Exchange instances (virtual servers) configured with VCS are marked as agentless managed and the cluster nodes are marked as agent managed. When a virtual server comes online on a node, the Lanman agent logs an alert that contains the name of the node on which the service group is online. The Helper Process utility detects this and switches the proxy to the node on which the Lanman resource is online. The Operations Manager 2007 server then starts querying the new proxy (node on which the virtual server is online) for events related to the virtual server.

Consider a 2-node VCS cluster, where Node1 and Node2 are the system names and INST1 is the clustered SQL instance (virtual server). Node1 and Node2 are configured as agent managed and INST1 is configured as agentless managed object. When INST1 is online on Node1, Operations Manager 2007 server retrieves INST1 related events from Node1. If INST1 fails over to Node2, all INST1 related events are logged in the Node2 event log. The Helper Process utility detects this information from the Lanman agent alert, and switches the proxy to Node2. The Operations Manager 2007 server now retrieves INST1 related events from the Node2 event log.

Thus, the Helper Process utility enables Operations Manager 2007 server to retrieve and monitor events related to the clustered SQL or Exchange instances, from the nodes (physical systems) on which they are online.

To install the Helper Process utility

- 1 From the Operations Manager 2007 server, navigate to the following directory on the product disc:

```
MOMPacks\cluster_server\storage_foundation_ha_for_windows\OPSMGR2007
```

- 2 Double-click **install.bat**. The Helper Process utility, *MOMHelper.exe*, is installed to the following directory on the Operations Manager server:

```
C:\Program Files\Symantec\MOMUtils\OpsMgr2007
```

Do not change the installation directory of the Helper Process utility.

Importing the VCS management packs

Use these procedures to import the VCS management packs in the Operations Manager 2007 server.

Before you proceed, ensure that:

- Verify that Operations Manager 2007 infrastructure is set up and configured correctly.
See the Microsoft System Center Operations Manager 2007 documentation for more information.
- If you have SQL configured, ensure that the SQL Server Browser service is running on all the nodes.
- Install SQL-DMO on all the nodes where SQL service group is configured.
Using SQL-DMO you can monitor the SQL Server 2008 instances.
See the Microsoft System Center Operations Manager 2007 documentation for more information.

Importing the base VCS management pack

Use the following procedure to import the base VCS management pack to monitor the VCS components.

To import the base VCS management pack

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 Management Group.
- 2 In the Operations Console, click **Administration**.
- 3 Right-click the **Management Packs** node and then click **Import Management Packs....**
- 4 In the Select Management Packs to import dialog box, navigate to the directory that holds the base VCS Management Pack file, click **Symantec.SFW.HA.mp** and then click **Open**.
- 5 In the Import Management Packs dialog box, select the base VCS management pack file (**Symantec.SFW.HA.mp**) from the list and click **Import**.
- 6 After the import process is complete, and the dialog box displays an icon next to the management pack indicating success or failure, click **Close**.
- 7 On successful import, the base VCS management pack is listed as *VCS for Windows by Symantec* in the Management Packs displayed in the Results pane.

Importing the VCS SQL or Exchange management pack

Use the following procedure to import the VCS SQL or Exchange management pack. The steps are the same for both SQL and Exchange.

Before you proceed, ensure that:

- You have imported the base VCS Management Pack.
See “[Importing the base VCS management pack](#)” on page 18 for more information.
- If you have SQL configured, ensure that the SQL Server Browser service is running on all the nodes.

To import the VCS SQL or Exchange management pack

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 Management Group.
- 2 In the Operations Console, click **Administration**.
- 3 Import the Microsoft Exchange or SQL management packs. If you have already imported the Microsoft management packs, proceed to the next step.
 - In the Administration pane, right-click **Management Packs** and then click **Import Management Packs...**
 - In the Select Management Packs to import dialog box, navigate to the directory that holds the Microsoft management pack files, select the appropriate files and then click **Open**.
For SQL 2000, select the following:
 - **Microsoft.SQLServer.2000.Discovery.mp**
 - **Microsoft.SQLServer.2000.Monitoring.mp**
 - **Microsoft.SQLServer.Library.mp**For SQL 2005, select the following:
 - **Microsoft.SQLServer.2005.Discovery.mp**
 - **Microsoft.SQLServer.2005.Monitoring.mp**
 - **Microsoft.SQLServer.Library.mp**For SQL 2008, select the following:
 - **Microsoft.SQLServer.2008.Discovery.mp**
 - **Microsoft.SQLServer.2008.Monitoring.mp**
 - **Microsoft.SQLServer.Library.mp**For Exchange 2003, select the following:
 - **Microsoft.Exchange.Server.2003.Discovery.mp**

- **Microsoft.Exchange.Server.2003.Monitoring.mp**

- **Microsoft.Exchange.Server.Library.mp**

For Exchange 2007, select the following:

- **Microsoft.Exchange.2007.mp**

- **Microsoft.Exchange.2007.Reporting.mp**

- In the Import Management Packs dialog box, select the appropriate Microsoft management packs from the list and click **Import**. You must select the files specified in the earlier step.
- After the import process is complete, and the dialog box displays an icon next to each management pack indicating success or failure, click **Close**.

On successful import, the Microsoft management packs are listed in the management packs displayed in the Results pane.

4 Import the VCS Exchange or SQL management packs.

- In the Administration pane, right-click **Management Packs** and then click **Import Management Packs...**

- In the Select Management Packs to import dialog box, navigate to the directory that holds the Microsoft management pack files, select the appropriate files and then click **Open**.

For SQL 2000, select the following:

- **Symantec.SQLServer.2000.mp**

For SQL 2005, select the following:

- **Symantec.SQLServer.2005.mp**

For SQL 2008, select the following:

- **Symantec.SQLServer.2008.mp**

For Exchange 2003, select the following:

- **Symantec.Exchange.Server.2003.mp**

For Exchange 2007, select the following:

- **Symantec.Exchange.Server.2007.mp**

- In the Import Management Packs dialog box, select the appropriate VCS management pack from the list and click **Import**. You must select the file specified in the earlier step.
- After the import process is complete, and the dialog box displays an icon next to each management pack indicating success or failure, click **Close**.

On successful import, the VCS management pack is listed in the management packs displayed in the Results pane.

Note that the above VCS Exchange or SQL management packs customizes and overwrites the following discoveries from the Microsoft Exchange or SQL management packs.

Table 2-1 Customized discoveries from Microsoft Exchange and SQL MOM packs

Application	Microsoft management pack discovery ID	VCS management pack discovery ID
SQL Server 2000	Microsoft.SQLServer.2000.DBEngineDiscoveryRule.Server	Symantec.SQLServer.2000.DBEngineDiscoveryRule.Server
SQL Server 2005	Microsoft.SQLServer.2005.DBEngineDiscoveryRule.Server	Symantec.SQLServer.2005.DBEngineDiscoveryRule.Server
SQL Server 2005	Microsoft.SQLServer.2005.ReportingServicesDiscoveryRule.Server	Symantec.SQLServer.2005.ReportingServicesDiscoveryRule.Server
SQL Server 2005	Microsoft.SQLServer.2005.AnalysisServicesDiscoveryRule.Server	Symantec.SQLServer.2005.AnalysisServicesDiscoveryRule.Server
SQL Server 2005	Microsoft.SQLServer.2005.IntegrationServicesDiscoveryRule.Server	Symantec.SQLServer.2005.IntegrationServicesDiscoveryRule.Server
SQL Server 2008	Microsoft.SQLServer.2008.DBEngineDiscoveryRule.Server	Symantec.SQLServer.2008.DBEngineDiscoveryRule.Server
SQL Server 2008	Microsoft.SQLServer.2008.ReportingServicesDiscoveryRule.Server	Symantec.SQLServer.2008.ReportingServicesDiscoveryRule.Server
SQL Server 2008	Microsoft.SQLServer.2008.AnalysisServicesDiscoveryRule.Server	Symantec.SQLServer.2008.AnalysisServicesDiscoveryRule.Server
SQL Server 2008	Microsoft.SQLServer.2008.IntegrationServicesDiscoveryRule.Server	Symantec.SQLServer.2008.IntegrationServicesDiscoveryRule.Server
Exchange 2003	Microsoft.Windows.Exchange.2003.InitalRegistryDiscovery	Symantec.Windows.Exchange.2003.InitalRegistryDiscovery

Table 2-1 Customized discoveries from Microsoft Exchange and SQL MOM packs

Application	Microsoft management pack discovery ID	VCS management pack discovery ID
Exchange 2007	Microsoft.Exchange.2007.Microsoft_Exchange_2007_Mailbox_Servers_Installation.Discovery	Symantec.Exchange.2007.Microsoft_Exchange_2007_Mailbox_Servers_Installation.Discovery
Exchange 2007	Microsoft.Exchange.2007.Microsoft_Exchange_2007_Mailbox_Servers_Physical_Computers_Installation.Discovery	Symantec.Exchange.2007.Microsoft_Exchange_2007_Mailbox_Servers_Physical_Computers_Installation.Discovery
Exchange 2007	Microsoft.Exchange.2007.Microsoft_Exchange_2007_Mailbox_Servers_CMS_and_Physical_Computer_Installation.Discovery	Symantec.Exchange.2007.Microsoft_Exchange_2007_Mailbox_Servers_CMS_and_Physical_Computer_Installation.Discovery

For Exchange 2007, in addition to the above mentioned discoveries, the VCS management pack also customizes and overwrites the following Microsoft management pack rules.

Table 2-2 Customized rules for Exchange 2007

Microsoft management pack discovery ID	VCS management pack discovery ID
Execute: Test-ExchangeSearch cmdlet	Execute: Test-ExchangeSearch cmdlet
Test-Mailflow (Local) diagnostic cmdlet (Report Collection)	Execute: Test-Mailflow (Local) diagnostic cmdlet (Report Collection) in VCS
Test-Mailflow (Remote) diagnostic cmdlet (Report Collection)	Execute: Test-Mailflow (Remote) diagnostic cmdlet (Report Collection) in VCS
Execute: Test-MAPIConnectivity diagnostic cmdlet (Report Collection)	Execute: Test-MAPIConnectivity diagnostic cmdlet (Report Collection) in VCS
Test-ServiceHealth diagnostic cmdlet	Execute: Test-ServiceHealth diagnostic cmdlet in VCS

Table 2-2 Customized rules for Exchange 2007

Microsoft management pack discovery ID	VCS management pack discovery ID
Test-SystemHealth diagnostic cmdlet	Execute: Test-SystemHealth diagnostic cmdlet in VCS

Note: For Microsoft Exchange 2007, the VCS management pack creates a new WriteActionModuleType "Microsoft_Exchange_2007__Execute_Diagnostic_Cmdlet_in_VCS". This is a modified version of Microsoft_Exchange_2007__Execute_Diagnostic_Cmdlet module.

Enabling VCS management pack monitoring

Complete this procedure to enable VCS management pack monitoring on physical systems that are part of the cluster.

To configure the VCS management packs

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 Management Group.

- 2 Create a Run as Account for the user to provide access to update MOM Server using MOM SDK.

You can also use the logged-on user account as Run As Account. In case you wish to use the logged-on user account as the Run as Account, skip this step and proceed to step 3.

To create the Run as Account, perform the following:

- In the Administration pane, under the Security options, right-click **Run as Accounts** and click **Create Run as Account**.
- On the Introduction panel of the Create Run as Account wizard, click **Next**.
- On the General panel, select the **account type**, enter the **display name** and **description** in the respective fields and then click **Next**.
- On the Account panel, type the **user name** and **password** and select the **domain** from the respective fields. Click **Create**.

Note that the user account must have access to update MOM server using MOM sdk.

- 3 Specify the Run as Account for the management servers, that manage the VCS Cluster nodes.

To specify the Run as Account for the management servers, perform the following:

- In the Administration pane, under the Security option, click **Run as Profiles**. The results pane displays all profiles that exists on the management server.
- In the results pane, right-click **MOMHelper profile** and click **Properties**.
- On the Run as Profile Properties panel, click **Run as Accounts** tab and click **New** to specify the Run as Account for the Management servers.
- On the Add Alternate Run as Account panel, select the desired account from the **Run as Account** drop-down list.
- Select the desired Management Server from the list of servers displayed in the Matching Computers grid. Click **Ok**.

- On the Run as Profiles Properties panel, click **Ok**.
- 4 Create a management pack.

In the Administration pane, right-click **Management Packs**, click **Create Management Pack** and complete the steps as per the Create a Management Pack wizard.

For sake of convenience, this management pack is referred as *OverridesMgmtPack* in this procedure.
 - 5 Create a physical server group, as follows:
 - In the Authoring pane, expand **Authoring**, right-click **Groups**, click **Create a new Group** to launch the Create Group Wizard.
 - In the General Properties pane, type a name for the Group and from the Select destination management pack drop-down list select the management pack, *OverridesMgmtPack*, that you created. Click **Next**.
 - In the Explicit Members pane, click **Next**.
 - In the Dynamic Members pane, click **Next**.
 - In the Subgroups pane, click **Next**.
 - In the Exclude Members pane, click **Create**.
 - 6 For the physical server group you created in the previous step, override the *Lanman Resource is Online* rule as follows:
 - In the Authoring pane, expand **Management Pack Objects**, and click **Rules**.
 - To see the VCS specific rules, click the **Change Scope** link and type VCS in the **Look for** text box, on the Scope Management Pack Objects by target(s) dialog box.
 - In the Scope Management Pack Objects by target(s) dialog box, click **Clear ALL**.
 - Select **VCS for Windows installation by Symantec** and then click **OK**.
 - In the Rules pane, type *Lanman* in the **Look for** text box, and then click **Find Now**. The Lanman resource is online rule appears in the Rules pane.
 - In the Rules pane, right-click the Lanman resource is online rule, and click **Overrides > Override the Rule > For a group**, and from the Select Object dialog box, select the physical server group that you created and then click **OK**.
 - In the Override Properties dialog box, select the **Override** check box, and select **True** from the Override Setting drop-down list.
 - Click **Apply** and then click **OK**.

- 7 For the Operations Manager 2007 server, override the VCS rule, *Call MOM Helper Utility*, as follows:
 - In the Authoring pane, expand **Management Pack Objects**, and click **Rules**. The results pane displays all the rules that are included in the management packs on the server.
 - To see VCS specific rules, at the top of the results pane, click **Change Scope....**
 - In the Scope Management Pack Objects by target(s) dialog box, click **Clear ALL**, select **Management Server** from the list of targets and then click **OK**.
 - Type **Call MOMHelper Utility** in the Look for: field and then click **Find Now**. The Call MOMHelper Utility rule is displayed in the Rules pane.
 - In the Rules pane, right-click the VCS rule *Call MOMHelper Utility*, click **Overrides > Override the Rule > For a specific object of type: Management Server**, and from the **Select a Target Type** dialog box, select the desired Management Server and then click **OK**.
 - In the Override Properties dialog box, select the **Override** check box, and select **True** from the Override Setting drop-down list.
 - In the Select destination management pack drop-down list, select the management pack, *OverridesMgmtPack* that you created in step 4.
 - Click **Apply** and then click **OK**.

Disabling additional monitoring for clustered instances

A management pack contains rules, monitors and other object discoveries that are set by the vendor of the management pack. A management pack begins monitoring a specific application as soon as it is imported. You may want to customize the default settings in these management packs to disable monitoring for clustered instances.

Let us consider an example where you are monitoring an application, *ApplicationX*, on a system, *System1*, using a third-party management pack. Install and configure Exchange with VCS on *System1*. Exchange in a VCS cluster environment works in the virtual server context. On importing the VCS management packs, computer objects *System1* and Exchange virtual server, *EVS1*, are displayed in the Operations Manager 2007 server. The third-party management pack monitors *ApplicationX* on *System1* and also on *EVS1* computer object. Similarly, the VCS management pack monitors Exchange on *EVS1* and also on *System1*.

In this case, you do not want the third-party management pack to monitor on *EVS1*, and the VCS management pack to monitor on *System1*. To accomplish

this, you can use overrides to disable additional monitoring for those management packs.

The following procedure describes how to override a VCS object discovery, *Symantec.SFW.HA.VCS_Windows_Installation.Discovery*, as an example. You must repeat this procedure to disable monitoring for the management packs from other vendors, as required.

To override management pack default settings

- 1 Create a virtual server group, as follows:
 - In the Operations Console, click **Authoring**, and in the Authoring pane, expand **Authoring**, right-click **Groups**, click **Create a new Group** to launch the Create Group Wizard.
 - In the General Properties pane, type a name for the group and from the Select destination management pack drop-down list select the management pack, *OverridesMgmtPack*. Click **Next**.
 - In the Explicit Members pane, click **Next**.
 - In the Dynamic Members pane, click **Next**.
 - In the SubGroups pane, click **Next**.
 - In the Excluded Members pane, click **Create**.
- 2 For the virtual server group that you created in step 1, override the object discovery *Symantec.SFW.HA.VCS_Windows_Installation.Discovery* for the base VCS management pack, as follows:
 - In the Authoring pane, expand **Management Pack Objects**, and then click the **Object Discoveries**.
 - To find the object discovery that you wish to override, click **Change Scope...** at the top of the results pane.
 - In the Scope Management Pack Objects by target(s) dialog box, click **Clear ALL**, select **VCS for Windows Installation by Symantec** and then click **OK**.
 - In the Object Discoveries pane, right-click the object discovery, *Symantec.SFW.HA.VCS_Windows_Installation.Discovery*, click **Overrides > Override the Rule > For a group...**, and from the Select Object dialog box, select the virtual server group and then click **OK**.
 - In the Override Properties dialog box, check the **Override** check box for the enabled attribute, and select **False** from the Override Setting drop-down list.
 - Click **Apply** and then click **OK**.

This disables the discovery, *Symantec.SFW.HA.VCS_Windows_Installation.Discovery*, for the empty Group.

- 3 If required, repeat step 2 to override rules, monitors, and other object discoveries of the other management packs for the virtual server group you created.

Configuring cluster nodes

Complete the following procedures.

Installing the Operations Manager 2007 agent

Complete this procedure to discover cluster nodes and deploy the Operations Manager 2007 agent to them from the Operations Manager 2007 console.

Note: Make sure the SQL or Exchange service group is not online on the node on which you are installing the agent. If the service group is online on the node, switch it to the failover node until the agent installation and proxy configuration settings are completed.

To install the Operations Manager 2007 agent

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 Management Group.
- 2 In the Operations Console, click **Administration**.
- 3 At the bottom of the navigation pane, click **Discovery Wizard....**
- 4 On the Introduction panel, click **Next**.
- 5 On the Auto or Advanced? panel, select either **Automatic computer discovery** or **Advanced discovery**. If you select Automatic computer discovery, click **Next**, and then go to [step 7](#). If you select Advanced discovery, continue with the following steps:
 - In the Computer & Device Types list, select **Servers & Clients**.
 - In the Management Server list, click the computer that you want to use to discover the computers.
 - Select the **Verify discovered computers can be contacted** check box. This is likely to increase the success rate of agent installation, but discovery can take longer.
 - Click **Next**.
- 6 On the Discovery Method panel, you can locate the computers that you want to manage by either scanning or browsing Active Directory Domain Services or typing the computer names.
If you want to scan, do the following:
 - If it is not already selected, select **Scan Active Directory** and then click **Configure**.

- In the Find Computers dialog box, type the desired criteria for discovering computers and then click **OK**.
- In the Domain list, click the domain of the computers that you want to discover.
- Click **Next**.

If you want to browse Active Directory or type the computer names, do the following:

- Select **Browse for, or type-in computer names**, click **Browse**, specify the names of the computers you want to manage, and then click **OK**.
- In the Browse for, or type-in computer names box, type the computer names, separated by semi-colon, comma, or a new line.
- Click **Next**.

7 On the Administrator Account panel, do one of the following:

- Select **Use selected Management Server Action Account** if it is not already selected.
- Select **Other user account**, type the User name and Password, and then select the Domain from the list. If the User name is not a domain account, select **This is a local computer account, not a domain account**. The account must have administrative privileges on the targeted computers. If you select **This is a local computer account, not a domain account**, the Management Server Action Account is used to perform discovery.

8 Click **Discover** to display the Discovery Progress panel.

9 On the Select Objects to Manage panel, do the following and then click **Next**:

- Select the cluster nodes on which you want to install the agent. You must select the cluster nodes using the physical name of the node, and not the virtual server name.
- From the Management Mode drop-down list, select **Agent**.

10 On the Summary page, do the following and then click **Finish**:

- Leave the Agent installation directory set to the default of %ProgramFiles%\System Center Operations Manager 2007 or type an installation path.
If a different Agent installation directory is specified, the root of the path must exist on the targeted computer or agent installation fails.
- Leave Agent Action Account set to the default, Local System, or select **Other** and type the User name, Password, and Domain. The Agent Action Account is the default account the agent uses to perform actions.

In the Agent Management Task Status box, the Status for each selected node changes to Success. This indicates that the agent is installed successfully.

- 11 Click **Close**. After the agent is installed, the node is added to the *Agent-Managed* group.

Configuring agent-managed computers as proxy

This procedure is required only if you plan to import the VCS SQL or Exchange management pack on the Operations Manager 2007 server.

After the Operations Manager 2007 agent installation, the cluster nodes are added to the *Agent Managed* group. Use the following procedure to configure these cluster nodes (agent-managed computers) as a proxy for virtual servers (agentless managed computers) that are running on these nodes. This enables the events generated by the clustered SQL or Exchange instances (virtual servers) to be reported to the Operations Manager 2007 server.

To configure agent-managed computers as proxy

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 Management Group.
- 2 In the Operations Console, click **Administration**.
- 3 In the Administration pane, expand **Administration**, expand **Device Management**, and then click **Agent Managed**.
- 4 In the results pane, right-click a cluster node and then click **Properties**.
- 5 In the Agent Properties dialog box, click the **Security** tab, select **Allow this agent to act as a proxy and discover managed objects and on other computers**, and then click **OK**.
- 6 Repeat steps 4 and 5 for the remaining nodes in the cluster.

Adding physical servers to the group created

Add clustered nodes to the group that you created in the procedure “[Enabling VCS management pack monitoring](#)” on page 24.

To add clustered nodes to the group created

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 Management Group.
- 2 In the Operations Console, click **Authoring**.

- 3 In the Authoring pane, expand **Authoring**, and then click **Groups**.
- 4 From the Groups pane, right-click the **Group** that you created earlier in “[Enabling VCS management pack monitoring](#),” and then click **Properties**.
- 5 In the Explicit Members pane, click **Add/Remove Objects...**, in the Object Selection dialog box, select **Windows Computer** from the Search for: drop-down list, and then click **Search** to search the SQL or Exchange physical systems.
- 6 Click **Apply** and then click **OK**.

Configuring clustered instances

Adding clustered instances as agentless-managed objects

SQL and Exchange in a VCS cluster environment work in the virtual server context. Events generated by SQL and Exchange instances are in the name of the virtual server. Similarly, service groups that include a Lanman resource (for example, File Share, Print Share) operate in the virtual server context. To be able to monitor these virtual servers, you must configure them as agentless managed.

Before you proceed, ensure that the Lanman resource is online on the cluster node. Also, ensure that the Lanman agent attributes, ADUpdateRequired and DNSUpdateRequired are set to True. If they are not, set them to True, take the Lanman resource offline and then bring it online.

To configure clustered instances as agentless managed computers

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 Management Group.
- 2 In the Operations Console, click **Administration**.
- 3 At the bottom of the navigation pane, click **Discovery Wizard...**
- 4 On the Introduction panel, click **Next**.
- 5 On the Auto or Advanced? panel, select **Advanced discovery**, complete the following and then click **Next**:
 - In the Computer & Device Types list, select **Servers & Clients**.
 - In the Management Server list, click to select the computer that you want to use to discover the computers.
 - Uncheck the **Verify discovered computers can be contacted** check box.
- 6 On the Discovery Method panel, do the following and then click **Next**:
 - In the Browse for, or type-in computer names box, type the SQL or Exchange virtual server names, separated by semi-colon, comma, or a new line.
- 7 On the Administrator Account panel, specify a user account with Administrative rights on the virtual computer and then click **Discover** to begin the discovery.
- 8 On the Select Objects to Manage panel, do the following and then click **Next**:
 - Select the virtual server names.
 - From the Management Mode drop-down list, select **Agentless**.

- In the Proxy Agent field select the cluster node on which the Lanman resource is online.
- 9 On the Summary panel, click **Finish**.
The virtual computers you specified are now added to the *Agentless Managed* group.

Adding clustered instances to the empty Group

In the procedure “[Disabling additional monitoring for clustered instances](#)” on page 26, you created an empty Group and then disabled the VCS object discovery, *Symantec.SFW.HA.VCS_Windows_Installation.Discovery*, and the override rules, monitors, and object discoveries of the other management packs, for this empty Group. We now add all the clustered instances to that empty Group. This ensures that the override rules, monitors, and object discoveries are disabled for these virtual server instances.

To add clustered instances to the empty Group

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 Management Group.
- 2 In the Operations Console, click **Authoring**.
- 3 In the Authoring pane, expand **Authoring**, and then click **Groups**.
- 4 From the Groups pane, right-click the empty Group that you created earlier and then click **Properties**.
- 5 On the Explicit Members tab, click **Add/Remove Objects...**, and in the Object Selection dialog box, select **Windows Computer** from the Search for: drop-down list, and then click **Search**. The virtual computers are displayed in the Available items list.
- 6 From the Available items, select the desired virtual computer, click **Add**, and then click **OK**.
- 7 Click **Apply** and then click **OK**.

Monitoring rules

This chapter contains the following topics:

- [“HAD monitoring rules”](#) on page 36
- [“GAB monitoring rules”](#) on page 65
- [“LLT monitoring rules”](#) on page 67
- [“Agents monitoring rules”](#) on page 68
- [“Enterprise application agents”](#) on page 101
- [“Agent Framework monitoring rules”](#) on page 123

About monitoring rules

This chapter lists the monitoring rules for VCS components, SQL Server, and Exchange server. The monitoring rules consist of event processing rules and alert processing rules.

HAD monitoring rules

[Table 3-1](#) lists the rules for the VCS High Availability Engine (HAD).

Table 3-1 HAD Monitoring Rules

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
10746	HAD	Incorrect snmp command	Warning	Y	N
10755	HAD	Unexpected return value	Warning	Y	N
10761	HAD	Node id expected	Warning	Y	N
10772	HAD	Too many options	Warning	Y	N
10792	HAD	Must specify the type name	Warning	Y	N
10799	HAD	Too few arguments	Warning	Y	N
10805	HAD	Connection timed out	Warning	Y	N
10806	HAD	Error while registering resource	Warning	Y	N
10809	HAD	Value type not supported	Warning	Y	N
10811	HAD	Invalid group dependency type specified: %1	Warning	Y	N
10813	HAD	Unable to open file '%1'. The file may be corrupted or does not exist.	Warning	Y	N
10814	HAD	Incorrect LDF path specified	Warning	Y	N
10815	HAD	Incorrect message severity specified	Warning	Y	N
10816	HAD	Incorrect object type specified	Warning	Y	N
10817	HAD	Incorrect object name specified	Warning	Y	N
10818	HAD	VCS object tag does not have an object name	Warning	Y	N
10819	HAD	Incorrect message ID specified	Warning	Y	N
10821	HAD	No messages match your query	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
10822	HAD	No log files available	Warning	Y	N
10823	HAD	Incorrect language specified	Warning	Y	N
10824	HAD	Unable to open file '%1'. This file was generated by a newer version of the VCS engine.	Warning	Y	N
10825	HAD	Tail value must be an integer value greater than 0	Warning	Y	N
10826	HAD	Incorrect system specified for checkpartial option	Warning	Y	N
11005	HAD	hacf -status died. Transitioning to STALE_DISCOVER_WAIT	Error	Y	N
11007	HAD	Exiting:Cannot lock %1 error = %2	Error	Y	N
11009	HAD	Exiting: Another copy of VCS may be running	Error	Y	N
11012	HAD	Cannot lock file: %1 error = %2	Warning	Y	N
11014	HAD	Cannot write '%1' to %2	Warning	Y	N
11015	HAD	Environment variable %1 is not defined	Error	Y	N
11016	HAD	Failed to interpret line %1	Error	Y	N
11021	HAD	Failed to notify service ctl manager (SCM)	Warning	Y	N
11024	HAD	System name retrieval failed	Warning	Y	N
11028	HAD	Error querying Registry value %1	Error	Y	N
11030	HAD	HAD not ready to receive this command. Message was: 0x%1	Warning	Y	N
11031	HAD	GABTCP open failed. Exiting.	Error	Y	N
11032	HAD	Registration failed. Exiting.	Error	Y	N
11033	HAD	GAB open failed. Exiting.	Error	Y	N
11036	HAD	GAB recv failed. Exiting.	Error	Y	N
11037	HAD	Failed to StartServiceCtrlDispatcher %1	Error	Y	N
11038	HAD	Failed to open had service	Error	Y	N
11039	HAD	Failed to make MSG_CLUSTER_STOP_SYS.	Error	Y	N
11041	HAD	Engine Stopping Deleting vlist for %1	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
11043	HAD	Unknown major/minor msg = %1	Warning	Y	N
11045	HAD	Unable to create temporary file	Warning	Y	N
11046	HAD	Local system not available	Warning	Y	N
11047	HAD	Unable to execute the hastatus print command	Warning	Y	N
11055	HAD	Unknown process-registration msg: %1	Warning	Y	N
11062	HAD	Group '%1' does not exist. Resources added later will not be registered.	Warning	Y	N
11064	HAD	Type '%1' does not exist. Resources added later will not be registered	Warning	Y	N
11084	HAD	%1 is an invalid TAG	Warning	Y	N
11086	HAD	Exiting: Cannot make directory: %1	Error	Y	N
11098	HAD	Another hashadow running. VCS engine is exiting.	Warning	Y	N
11103	HAD	VCS exited. It will restart .	Error	Y	N
11104	HAD	VCS has faulted %1 times since %2 hashadow will not restart VCS. Correct the problem and restart VCS.	Error	Y	N
11106	HAD	Cannot get lock on file: %1	Warning	Y	N
11108	HAD	Cannot start had. Error=0x%1	Warning	Y	N
11109	HAD	Cannot start had. Error=%1	Warning	Y	N
11113	HAD	Memory allocation failed.	Warning	Y	N
11130	HAD	No username.	Warning	Y	N
11131	HAD	Incorrect username.	Warning	Y	N
11135	HAD	Cannot get password -- error 0x%1	Warning	Y	N
11137	HAD	Cannot encrypt password -- error 0x%1	Warning	Y	N
11148	HAD	Cannot ioctl(IOCTL_LLT_GETPARAM/LP_MAXLINKS (Windows Error Code = %1)	Warning	Y	N
11149	HAD	Cannot ioctl(IOCTL_LLT_GETLINKINFO (Windows Error Code = %1)	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
11150	HAD	Cannot ioctl(IOCTL_LLTT_GETPARAM/LP_MAXNODE (Windows Error Code = %1)	Warning	Y	N
11151	HAD	Cannot ioctl(IOCTL_LLTT_GETNODEALL (Windows Error Code = %1)	Warning	Y	N
11152	HAD	Cannot malloc(%1 for msgbuf)	Warning	Y	N
11154	HAD	Cannot ioctl(IOCTL_LLTT_GETPARAM/LP_MAXNODE)	Warning	Y	N
11164	HAD	Cannot ioctl(IOCTL_LLTT_GETNODEALL)	Warning	Y	N
11165	HAD	Error opening /dev/gab_0	Warning	Y	N
11166	HAD	Error opening /dev/llt	Warning	Y	N
11168	HAD	Cannot ioctl(IOCTL_LLTT_GETLINKINFO)	Warning	Y	N
11169	HAD	Failed to get Link heartbeat status.	Error	Y	N
11170	HAD	Failed to get Disk heartbeat status.	Error	Y	N
11171	HAD	Cannot ioctl(IOCTL_LLTT_GETPARAM/LP_MAXLINKS)	Warning	Y	N
11274	HAD	System shutting down on %1	Error	Y	N
11277	HAD	Retry Interval is %1 at fault %2	Warning	Y	N
11278	HAD	Error on executing gab_getdisk.	Warning	Y	N
11279	HAD	Failed to read file '%1'	Warning	Y	N
11280	HAD	hadiscover could not find function (%1) in library	Warning	Y	N
11281	HAD	Discovery of %1 attribute failed	Warning	Y	N
11282	HAD	Failed to list discoverable attributes	Warning	Y	N
11283	HAD	Discovery not supported for Type %1	Warning	Y	N
11284	HAD	Your evaluation period has expired. VCS will not start the next time you invoke hastart	Warning	Y	N
11285	HAD	[Licensing] You have %1 day(s) left in your VCS evaluation period	Error	Y	N
11286	HAD	Updating license key on %1	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
11287	HAD	Failed to update engine's copy of license key	Error	Y	N
11288	HAD	License key updated successfully on the local node. The halic utility needs to be run on all nodes in the cluster in order for the VCS license to be updated properly	Warning	Y	N
11289	HAD	License key is not unique within cluster. Failed to update license key.	Error	Y	Y
11290	HAD	WARNING:One or more systems are not online.	Warning	Y	N
11291	HAD	Canceling license key update	Warning	Y	N
11292	HAD	WARNING:halic is unable to determine whether or\nnot this key is unique within the cluster. Duplicate keys\nwill prevent nodes from rejoining the cluster.\n\nDo you wish to continue? [Y/N]:	Warning	Y	N
11300	HAD	User name is a reserved word or contains invalid character(s)	Error	Y	Y
11301	HAD	System can not be restarted: err:%1	Error	Y	Y
11303	HAD	Exiting: HAD has encountered a critical error. Please check VCS_HOME/log/drwatson for logs	Error	Y	Y
11304	HAD	Please enter valid English arguments	Warning	Y	N
11309	HAD	Configuration must be ReadWrite	Warning	Y	N
11316	HAD	User name should be of the format user@domain	Error	Y	Y
11317	HAD	'%1' is an invalid debug log tag.	Warning	Y	N
11318	HAD	Cannot specify both -sev and -dbg	Warning	Y	N
11319	HAD	The -parameters option must be the last option specified	Warning	Y	N
11320	HAD	Must also specify -parameters when using the -encoding option	Warning	Y	N
11321	HAD	Invalid message specified	Warning	Y	N
11322	HAD	Invalid system specified	Warning	Y	N
11323	HAD	Invalid severity specified	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
11325	HAD	Invalid debug level specified	Warning	Y	N
11327	HAD	Message ID must be under 65535	Warning	Y	N
11328	HAD	Invalid message ID specified	Warning	Y	N
11329	HAD	Invalid encoding specified	Warning	Y	N
11330	HAD	Invalid parameters specified	Warning	Y	N
11331	HAD	Exiting:Cannot register with SCM(service ctl manager) .err: %1.	Error	Y	Y
12021	HAD	Error - %1 (%2) in file %3:%4	Warning	Y	N
12022	HAD	Failed to get working directory	Warning	Y	N
12023	HAD	Unsuccessful open of ipm service	Warning	Y	N
12025	HAD	%1 %2 has an Administrators/Operators list without any users defined	Warning	Y	N
12026	HAD	Types file should have a .%1 extension	Warning	Y	N
12027	HAD	Cannot mkdir %1	Warning	Y	N
12028	HAD	Cannot chdir %1	Warning	Y	N
12029	HAD	%1 does not have a list	Warning	Y	N
12030	HAD	Cannot open lock file: errno = %1	Warning	Y	N
12031	HAD	Configuration locked	Warning	Y	N
12032	HAD	Cannot create file: %1	Warning	Y	N
12033	HAD	Cannot open file: %1	Warning	Y	N
12034	HAD	User %1 in %2 %3 %4	Warning	Y	N
12035	HAD	Error deleting file: %1	Warning	Y	N
12036	HAD	Source file should have a .%1 extension	Warning	Y	N
12037	HAD	Incorrect syntax for value of attribute SourceFile for type %1 : %2	Warning	Y	N
12038	HAD	Exiting: Cannot chdir %1.	Error	Y	Y
12039	HAD	Cannot open file: %1 error = %2	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
12040	HAD	Failed to change to working directory	Warning	Y	N
12041	HAD	Keyword i18nstr found : %1\nLocalized input not allowed.	Warning	Y	N
12043	HAD	Failed to dump the configuration from the live engine	Warning	Y	N
12046	HAD	Configuration stale	Warning	Y	N
12047	HAD	Cannot fork %1	Warning	Y	N
12048	HAD	Destination file should have a .%1 extension	Warning	Y	N
12051	HAD	Illegal group dependency clause	Warning	Y	N
12054	HAD	Cannot open input file: %1	Warning	Y	N
12055	HAD	Unexpected EOF: %1	Warning	Y	N
12056	HAD	Parent resource %1 does not exist %2	Warning	Y	N
12057	HAD	Child resource %1 does not exist %2	Warning	Y	N
12058	HAD	Unknown type %1 %2	Warning	Y	N
12059	HAD	Expecting -keys	Warning	Y	N
12060	HAD	Cannot find attribute %1	Warning	Y	N
12061	HAD	Scalar attributes cannot have multiple values	Warning	Y	N
12062	HAD	Cannot find resource %1	Warning	Y	N
12065	HAD	Unknown subcommand %1	Warning	Y	N
12066	HAD	Not enough arguments	Warning	Y	N
12071	HAD	Unexpected attribute %1	Warning	Y	N
12076	HAD	Cannot find group %1	Warning	Y	N
12083	HAD	Cannot find system %1	Warning	Y	N
12085	HAD	Expecting haevent -add	Warning	Y	N
12086	HAD	Unknown event %1	Warning	Y	N
12087	HAD	Unknown command %1	Warning	Y	N
12088	HAD	Unknown event subcommand %1	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
12089	HAD	Unexpected message: %1	Warning	Y	N
12090	HAD	Unknown message: %1	Warning	Y	N
12092	HAD	Ipm send failure	Warning	Y	N
12093	HAD	Recv failure	Warning	Y	N
12095	HAD	Aborting hacf: errors encountered	Warning	Y	N
12097	HAD	Duplicate definition for %1 at %2:%3	Warning	Y	N
12102	HAD	Parent resource %1 and child resource %2 do not belong to the same group	Warning	Y	N
12103	HAD	Cannot find attribute def for %1.%2	Warning	Y	N
12104	HAD	Expecting a list for %1	Warning	Y	N
12105	HAD	Cannot open output %1	Warning	Y	N
12109	HAD	Ipm sendrecv failure	Warning	Y	N
12111	HAD	Configuration may contain only one cluster clause	Warning	Y	N
12113	HAD	System %1 defined more than once	Warning	Y	N
12114	HAD	Group %1 defined more than once	Warning	Y	N
12115	HAD	Group %1 cannot have more than one group dependency clause	Warning	Y	N
12116	HAD	Group %1 has a local attribute without a SystemList	Warning	Y	N
12117	HAD	System %1 not on SystemList of group %2	Warning	Y	N
12120	HAD	Qualified name not found	Warning	Y	N
12121	HAD	Value for attribute %1 not found	Warning	Y	N
12122	HAD	Reserved word - %1 - cannot be used to name objects or attributes	Warning	Y	N
12123	HAD	Type %1 defined more than once	Warning	Y	N
12127	HAD	Cannot find group %1 %2	Warning	Y	N
12128	HAD	Resource %1 is %2 and must not have children	Warning	Y	N
12129	HAD	Resource %1 in a cycle	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
12130	HAD	Group %1 does not exist	Warning	Y	N
12131	HAD	Group %1 contains group dependency cycles	Warning	Y	N
12133	HAD	Group %1 contains too deep group dependency	Warning	Y	N
12134	HAD	SystemList for group %1 contains non-existent system %2	Warning	Y	N
12135	HAD	Group %1 has an AutoStartList without a SystemList	Warning	Y	N
12136	HAD	System %1 in the AutoStartList of group %2	Warning	Y	N
12137	HAD	Invalid Resource Type %1 in group %2	Warning	Y	N
12138	HAD	Cannot find type %1	Warning	Y	N
12139	HAD	Resource Type %1 occurring more than once in dependency attribute for group %2	Warning	Y	N
12140	HAD	Group %1 has SystemZones without a SystemList	Warning	Y	N
12141	HAD	System %1 in the SystemZones of group %2	Warning	Y	N
12142	HAD	Attribute %1 for %2 cannot be specified both local and global	Warning	Y	N
12143	HAD	Attribute %1 for %2 specified local on %3 more than once	Warning	Y	N
12144	HAD	Reserved word - %1 - cannot be used to name objects or attributes: %2	Warning	Y	N
12145	HAD	SystemList does not have a list	Warning	Y	N
12146	HAD	Group %1 has a local attribute %2 without SystemList	Warning	Y	N
12148	HAD	Local system not specified for %1 in group %2	Warning	Y	N
12149	HAD	Local system was specified for non local attribute %1 in group %2	Warning	Y	N
12150	HAD	Duplicate event item name %1 %2	Warning	Y	N
12151	HAD	Duplicate event name %1 %2	Warning	Y	N
12155	HAD	Bad include line in file %1:%2	Warning	Y	N
12156	HAD	No group defined	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
12158	HAD	AutoStartList does not have a list	Warning	Y	N
12159	HAD	Unable to get list of types files from VCS engine	Warning	Y	N
12160	HAD	Single slash not allowed	Warning	Y	N
12161	HAD	Quotes mismatch	Warning	Y	N
12162	HAD	Unexpected group dependency	Warning	Y	N
12163	HAD	No name given for cluster	Warning	Y	N
12164	HAD	No name given for group	Warning	Y	N
12165	HAD	No name given for system	Warning	Y	N
12166	HAD	No name given for type	Warning	Y	N
12167	HAD	Cannot change file permissions of %1	Warning	Y	N
12168	HAD	Cannot find HeartBeat %1	Warning	Y	N
12169	HAD	Attempting to add Remote Cluster %1. It is already the existing local cluster	Warning	Y	N
12170	HAD	Attempting to add Cluster %1. It is already an existing remote cluster	Warning	Y	N
12171	HAD	Heartbeat %1 is defined more than once	Warning	Y	N
12172	HAD	Remote Cluster %1 is defined more than once	Warning	Y	N
12173	HAD	Remote Cluster name %1 is same as the local cluster name	Warning	Y	N
12174	HAD	No name given for heartbeat	Warning	Y	N
12175	HAD	No name given for Remote Cluster	Warning	Y	N
12177	HAD	Cluster %1 defined in ClusterList of Heartbeat %2 is not a remote cluster	Warning	Y	N
12178	HAD	Local Cluster name and value of Cluster attribute ClusterName must be the same	Warning	Y	N
12180	HAD	Must specify name and IP address of Remote Cluster to be added	Warning	Y	N
12181	HAD	Remote Cluster Name missing	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
12182	HAD	%1 is not an existing Remote Cluster	Warning	Y	N
12183	HAD	Cannot override attribute %1	Warning	Y	N
12184	HAD	ClusterList of heartbeat %1 does not have a list	Warning	Y	N
12185	HAD	Heartbeat %1 has a local attribute %2 without ClusterList	Warning	Y	N
12186	HAD	Cluster %1 not on ClusterList of heartbeat %2	Warning	Y	N
12187	HAD	Cluster %1 defined in ClusterList of Group %2 is not a local or remote cluster	Warning	Y	N
12188	HAD	ClusterList for group %1 does not have a list	Warning	Y	N
12189	HAD	Cluster-scope not specified for local attribute %1 in heartbeat %2	Warning	Y	N
12190	HAD	Cluster-scope was specified for global attribute %1 in heartbeat %2	Warning	Y	N
12191	HAD	Line %1 of file %2 is not in UTF-8 format	Warning	Y	N
12193	HAD	Undefined Type : %1 %2	Warning	Y	N
12194	HAD	Mandatory attribute Missing : %1.%2	Warning	Y	N
12196	HAD	Configuration does not contain a Heartbeat object	Warning	Y	N
12197	HAD	Group %1 has a local hard dependency with level more than 1	Warning	Y	N
12198	HAD	Group %1 has multiple local hard parents	Warning	Y	N
12199	HAD	%1 and %2 cannot have the same ClusterAddress	Warning	Y	N
12200	HAD	ClusterAddress not defined for %1	Warning	Y	N
12201	HAD	No name given for resource : %1	Warning	Y	N
12202	HAD	Duplicate system name in SystemList of %1	Warning	Y	N
12203	HAD	Group ClusterService cannot have any parent group	Warning	Y	N
12207	HAD	Group ClusterService cannot have any child group	Warning	Y	N
12208	HAD	Group %1 : ClusterFailOverPolicy should be one of Manual	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
12210	HAD	Group %1 : Authority should be either 0 or 1	Warning	Y	N
12211	HAD	IPM Receive Error	Warning	Y	N
12212	HAD	IPM Protocol Error	Warning	Y	N
12213	HAD	Attribute %1 for %2 specified more than once	Warning	Y	N
12214	HAD	IPM Send Error	Warning	Y	N
12216	HAD	Insufficient space in %1 for temporary files	Warning	Y	N
12217	HAD	Failed to open temporary files	Warning	Y	N
12218	HAD	Could not create temporary files in %1	Warning	Y	N
12219	HAD	Error encountered while writing temporary files : %1	Warning	Y	N
12221	HAD	Cannot open file specified in the include statement: %1	Warning	Y	N
12222	HAD	Invalid IP address assigned to ClusterAddress of remote cluster %1	Warning	Y	N
12223	HAD	Group %1 depends on a non-existing group : %2	Warning	Y	N
13310	HAD	Offlining parent group %1 on system %2	Warning	Y	N
13326	HAD	Cannot find attribute(%1) in the resource type description	Error	Y	N
13327	HAD	Cannot find attribute(%1) in the resource attribute list	Error	Y	N
13332	HAD	Unable to update attribute ResourceInfo\n	Warning	Y	N
13338	HAD	Usage error	Warning	Y	N
13340	HAD	System name should be specified with cluster	Warning	Y	N
13341	HAD	Incorrect arguments to action	Warning	Y	N
13342	HAD	No overridden attributes	Warning	Y	N
13344	HAD	No overridden attributes in resources	Warning	Y	N
13345	HAD	No overridden attributes in resources	Warning	Y	N
13346	HAD	No overridden attributes in resources	Warning	Y	N
13347	HAD	No overridden attributes in any resource	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
13350	HAD	Cannot specify type/group/attribute/system as values for any of the options to the display command.	Warning	Y	N
13351	HAD	Invalid option: %1	Warning	Y	N
13352	HAD	Usage error: Value missing for option %1	Warning	Y	N
13357	HAD	Error in converting the input string into UCS-2 encoding. Output may be truncated	Warning	Y	N
13358	HAD	Error in converting the input string into UTF-8 encoding. Output may be truncated	Warning	Y	N
13463	HAD	Resource %1 does not belong to types(%2)\n	Warning	Y	N
13464	HAD	Resource %1 does not belong to groups(%2) \n	Warning	Y	N
13465	HAD	Resource %1 does not belong to types(%2) or groups(%3) \n	Warning	Y	N
13466	HAD	No overridden attributes in resources %1 or no resource in (%2) belongs to type(s) %3\n	Warning	Y	N
13467	HAD	No overridden attributes in resources %1 or no resource in (%2) belongs to group(s) %3\n	Warning	Y	N
13468	HAD	No overridden attributes in resources %1 or no resource in (%2) belongs to type(s) %3 and group(s) %4	Warning	Y	N
13469	HAD	No overridden attributes in resources %1	Warning	Y	N
14001	HAD	Config file %1 does not exist. Forming a one node cluster	Error	Y	N
14002	HAD	Node config file %1 does not exist. Forming a one node cluster	Error	Y	N
14005	HAD	Nodeid is %1. Forming a onenode cluster and setting nodeid to 0	Warning	Y	N
14007	HAD	Unsuccessful open of service %1	Error	Y	N
14016	HAD	Heartbeat did not contain 6 fields	Warning	Y	N
14017	HAD	Eject myself: Detected mynodeid in membership %1	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
14020	HAD	Deleting ipmhandle: No heartbeats received from nodeid %1 on link %2 current time = %3 past time = %4	Error	Y	N
14021	HAD	ioctl error while registering IP address %1	Warning	Y	N
16007	HAD	Failed to execute process: %1. Errno is %2	Warning	Y	N
16008	HAD	Failed to create process: %1. Errno is %2	Warning	Y	N
16009	HAD	Error in executing command: %1. Errno is %2	Warning	Y	N
17001	HAD	Notifier:Expected SNMP managers machine name	Warning	Y	N
17002	HAD	Notifier:Severity out of range	Warning	Y	N
17003	HAD	Notifier:Unexpected option	Warning	Y	N
17004	HAD	Notifier:Expected SMTP server name	Warning	Y	N
17005	HAD	Notifier:Expected mail recipients name	Warning	Y	N
17006	HAD	Notifier:Expected SNMP and or SMTP options	Warning	Y	N
17007	HAD	Notifier:exit by NOTIFIER_DISCONNECT msg. Connected to %1	Warning	Y	N
17009	HAD	Notifier:cannot connect to ipmserver	Warning	Y	N
17010	HAD	Notifier:cannot create thread	Warning	Y	N
17011	HAD	Notifier:cannot communicate to VCS	Warning	Y	N
17012	HAD	Notifier:send MSG_NOTIFIER_CONNECT failure	Warning	Y	N
17013	HAD	Notifier:IPM connection failed	Warning	Y	N
17014	HAD	Notifier:exit by NOTIFIER_DISCONNECT msg. Connected to unknown host	Warning	Y	N
17015	HAD	Notifier:receive messages unknown minor	Warning	Y	N
17016	HAD	Notifier:send MSG_NOTIFIER_ACK failed	Warning	Y	N
17017	HAD	Notifier:receive unknown message from VCS	Warning	Y	N
17018	HAD	Notifier:cannot create PDU for snmp trap	Warning	Y	N
17019	HAD	Notifier:cannot get local IP address	Warning	Y	N
17020	HAD	Notifier:cannot create snmp trap OID	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
17021	HAD	Notifier:cannot allocate memory for %1	Warning	Y	N
17022	HAD	Notifier:%1 undefined	Warning	Y	N
17023	HAD	Notifier:%1 command failure	Warning	Y	N
17024	HAD	Notifier:wrong service group type	Warning	Y	N
17025	HAD	Notifier:wrong heartbeat type	Warning	Y	N
17026	HAD	Notifier:cannot open snmp session to %1	Warning	Y	N
17027	HAD	Notifier:cannot send snmp trap	Warning	Y	N
17028	HAD	Notifier:cannot close snmp session	Warning	Y	N
17029	HAD	Notifier:unknown error	Warning	Y	N
17030	HAD	Notifier:cannot verify recipient %1	Warning	Y	N
17031	HAD	Notifier:activated signal %1	Warning	Y	N
17032	HAD	Notifier:send MSG_NOTIFIER_DISCONNECT failed	Warning	Y	N
17033	HAD	Notifier:cannot get snmp traps up time	Warning	Y	N
17034	HAD	Notifier:SNMP error %1	Warning	Y	N
17035	HAD	Notifier:SNMP unknown error	Warning	Y	N
17036	HAD	Notifier:SMTP error %1	Warning	Y	N
17037	HAD	Notifier:SMTP unknown error	Warning	Y	N
17038	HAD	Notifier:value of option %1 is out of range	Warning	Y	N
17039	HAD	Notifier:unknown trap ID	Warning	Y	N
17040	HAD	Notifier:unknown entities type	Warning	Y	N
17041	HAD	Notifier:unknown entities subtype	Warning	Y	N
17042	HAD	Notifier:options wrong order. Entity type must be define before entity subtypes	Warning	Y	N
17043	HAD	Notifier:send MSG_NOTIFIER_NOTIFY failure	Warning	Y	N
17045	HAD	Notifier:response to MSG_NOTIFIER_ALIVE failure	Warning	Y	N
17046	HAD	Notifier:%1 command failure for %2	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
17047	HAD	Notifier:Setting message Queue size to default value as value specified is less than default	Warning	Y	N
17049	HAD	Notifier:Message %1 is being deleted since message cannot be delivered for more than a hour	Warning	Y	N
17050	HAD	Notifier:Unhandled exception occurred	Warning	Y	N
17051	HAD	Notifier:Unable to connect to %1	Warning	Y	N
17053	HAD	Notifier:Mail server specified does not support SMTP VRFY command. Email user cannot be verified	Warning	Y	N
40000	HAD	ULF_CLI ULF_AGT	Error	Y	N
40001	HAD	Cannot connect to VCS simulator	Warning	Y	N
40002	HAD	Passwords do not match	Error	Y	N
40004	HAD	Error: Nodeid(%1 should be less than maxnodes(%2 This node cannot join the cluster	Error	Y	N
40006	HAD	Error: Cannot Initialize Socket	Error	Y	N
40007	HAD	Error: Unsuccessful open of service	Error	Y	N
40009	HAD	Unable to specify -status from the command line. %1	Warning	Y	N
40016	HAD	Error: invalid type %c	Error	Y	N
40024	HAD	Passwords do not match enter again	Error	Y	N
40103	HAD	On the FAULTED cluster %1	Warning	Y	N
40113	HAD	%1 %2	Warning	Y	N
40114	HAD	%1 %2 %3	Warning	Y	N
40115	HAD	Cannot specify both -localclus and -clus options	Warning	Y	N
40116	HAD	-localclus should be the last option.	Warning	Y	N
40125	HAD	No records found matching the specified conditions\n	Warning	Y	N
49001	HAD	Could not copy the sample configuration files	Error	Y	N
49002	HAD	Cannot find VCS_SIMULATOR_HOME	Error	Y	N
49003	HAD	Cannot gather Simulator port configurations for cluster %1	Error	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
49004	HAD	Port specified is already configured in this configuration.	Error	Y	N
49007	HAD	Configuration files created but could not update the simconfig file.	Error	Y	N
49008	HAD	Cannot find default simulator configuration.	Error	Y	N
49009	HAD	Directory for the specified cluster already exists. Cannot continue to configure.	Error	Y	N
49015	HAD	Cannot write to file: %1	Error	Y	N
49017	HAD	Simulator is already running on port '%1' for cluster '%2'.	Error	Y	N
49018	HAD	Could not find port information for the cluster %1. Specified cluster may not be configured.	Error	Y	N
49019	HAD	Could not connect to the cluster %1. It may not be Running.	Error	Y	N
49020	HAD	Could not stop SimServer. Error reported: %1	Error	Y	N
49021	HAD	Cannot gather cluster name information for port %1	Error	Y	N
50000	HAD	Group %1's prerequisites have not been fully met on system %2	Warning	Y	N
50007	HAD	Initiating auto-start online of group %1	Warning	Y	N
50016	HAD	Setting SYSSTATE to RSM_EXITED for node : %1.	Error	Y	N
50018	HAD	process_cluster() - received MSG_CLUSTER_DIE_DUPLICATE_NAME from node: %1. Will Exit now.	Warning	Y	N
50036	HAD	There are no enabled resources in the group %1 to online	Warning	Y	N
50039	HAD	Disabled resource: %1 can not be onlined	Error	Y	N
50040	HAD	All the resources in group are not completely offline	Error	Y	N
50043	HAD	For system %1 LLTNodeId:%2 and NodeId:%3 do not match	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
50044	HAD	For system %1 check if llftab file has correct set-node entry with reference to the llthosts file. VCS engine will exit to prevent any inconsistency	Warning	Y	N
50045	HAD	Initiating online of parent group %s	Warning	Y	N
50046	HAD	Initiating online of parent group %1 on node %2	Warning	Y	N
50047	HAD	Clearing parent group %1's migrateq	Warning	Y	N
50048	HAD	Migrating child %1 from node %2	Warning	Y	N
50049	HAD	Initiating online of child group %1	Warning	Y	N
50050	HAD	Migrating parent %s from node %1	Warning	Y	N
50051	HAD	Failed to read GAB message %1 time(s) due to insufficient memory.	Error	Y	N
50052	HAD	Insufficient memory to read GAB message. Panic system.	Error	Y	N
50053	HAD	Insufficient memory to read GAB message. Exiting.	Error	Y	N
50100	HAD	Command (%1) failed. Cluster Administrator or Group Administrator privilege required	Error	Y	N
50101	HAD	Command (%1) failed. Cluster Administrator privilege required	Error	Y	N
50102	HAD	Command (%1) failed. At least Cluster Operator privilege required	Error	Y	N
50103	HAD	Command (%1) failed. At least Group Administrator privilege required	Error	Y	N
50104	HAD	Command (%1) failed. At least Group Operator privilege required	Error	Y	N
50105	HAD	Command (%1) failed. User should be a %2	Warning	Y	N
50112	HAD	hacli is disabled	Warning	Y	N
50114	HAD	Invalid value %1 for key %2	Warning	Y	N
50115	HAD	Invalid value %1 for key %2	Warning	Y	N
50116	HAD	Invalid value %1 for key %2	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
50117	HAD	Invalid value %1 for key %2 can not modify key for this value	Warning	Y	N
50118	HAD	%1 is not a valid key for CPUUsageMonitoring	Warning	Y	N
50119	HAD	Error in disabling CPUUsage monitoring: %1	Error	Y	N
50120	HAD	Error in enabling CPUUsage monitoring: %1	Error	Y	N
50121	HAD	Error in reading CPUUsage: %1	Error	Y	N
50122	HAD	Invalid CPUUsage obtained: %1	Error	Y	N
50123	HAD	CPUUsage: %1 exceeded ActionThreshold: %2 on system %3	Error	Y	N
50124	HAD	CPUUsage: %1 exceeded NotifyThreshold: %2 on system %3	Warning	Y	N
50126	HAD	Group %1 is not yet fully probed on system %2	Warning	Y	N
50132	HAD	User %1	Warning	Y	N
50134	HAD	User %1	Warning	Y	N
50138	HAD	Some resources are in ADMIN WAIT state on system %1	Warning	Y	N
50141	HAD	Clearing the migrateq for parent group %1	Warning	Y	N
50148	HAD	ADMIN_WAIT flag set for resource %1 on system %2 with the reason %3	Error	Y	N
50300	HAD	Unsuccessful get of PDRs (%1)	Error	Y	N
50301	HAD	Unsuccessful in getting PD attributes (%1)	Warning	Y	N
50302	HAD	Unsuccessful search for non-root domain.	Error	Y	N
50303	HAD	Unsuccessful creation of private domain in Authentication Broker for VCS Engine(%1) %2	Error	Y	N
50304	HAD	Unsuccessful in getting Private Domain attributes (%1)	Error	Y	N
50305	HAD	Unsuccessful creation of Principal in Authentication Broker for VCS Engine(%1)	Error	Y	N
50307	HAD	Failed to initialize secure communication library (%1)	Error	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
50309	HAD	Security ON. Init failed. Clients will be rejected	Error	Y	N
50312	HAD	Unable to get FQDN for host (%1)	Error	Y	N
50505	HAD	Remote cluster %1 cannot be deleted as it is in the %2 state	Error	Y	N
50506	HAD	Remote cluster %1 cannot be deleted as it is a part of the clusterlist for group %2	Error	Y	N
50507	HAD	Remote cluster %1 cannot be deleted as it is a part of the clusterlist for heartbeat %2	Error	Y	N
50523	HAD	Number of clusters in the ClusterList attribute for group %1 is different between clusters %2 and %3	Error	Y	N
50524	HAD	Cluster %1 does not exist in the ClusterList attribute for group %2 in cluster %3	Error	Y	N
50526	HAD	Group %1's ClusterList priority for cluster %2 is different between clusters %3 and %4	Error	Y	N
50528	HAD	ClusterList values for global group %1 differ between the clusters. Not attempting to online group in local cluster	Error	Y	N
50529	HAD	Remote cluster %1 does not exist in the ClusterList attribute for group %2 in local cluster %3	Error	Y	N
50530	HAD	Group %1's ClusterList priority for cluster %2 is different between local cluster %3 and remote cluster %4	Error	Y	N
50531	HAD	Number of clusters in the ClusterList attribute for group %1 is different between local cluster %2 and remote cluster %3	Error	Y	N
50624	HAD	Simulator switched local system to %1	Warning	Y	N
50625	HAD	System (%1) is already up	Warning	Y	N
50626	HAD	Cannot bring system %1 up	Error	Y	N
50627	HAD	Cannot bring system %1 up	Error	Y	N
50628	HAD	System %1 is the last running node in the cluster. Stop the cluster instead of powering off this system	Warning	Y	N

Table 3-1 HAD Monitoring Rules (Continued)

Event ID	Module name	Rule Name	Severity	Event Enabled	Alert Enabled
50702	HAD	Remote cluster name needs to be specified.\n	Warning	Y	N
50704	HAD	Incorrect remote cluster specified	Warning	Y	N
50705	HAD	Must specify a system name	Warning	Y	N
50706	HAD	Incorrect cluster specified	Warning	Y	N
50710	HAD	Incorrect option	Warning	Y	N
50711	HAD	Insufficient arguments	Warning	Y	N
50712	HAD	Bad parameter	Warning	Y	N
50713	HAD	Specify one remote cluster	Warning	Y	N
50714	HAD	Please specify the heartbeat and attribute name.	Warning	Y	N
50717	HAD	Must specify a system name or use the -all option	Warning	Y	N
50727	HAD	Unexpected message 0x%1 while processing alerts from engine	Warning	Y	N
50728	HAD	Invalid alert ID specified	Warning	Y	N
50729	HAD	Invalid description specified	Warning	Y	N
50731	HAD	Incorrect category ID specified	Warning	Y	N
50739	HAD	Need to specify a description of why alert is being deleted	Warning	Y	N
50743	HAD	ClusterService group is not properly configured on cluster %1	Warning	Y	N
50757	HAD	Remote cluster %1 does not have Authority for global group %2. Not attempting to online in local cluster	Error	Y	N
50758	HAD	Not initiating online of parent group %1 after child online because parent group is in deferred AutoStart	Warning	Y	N
50759	HAD	Not initiating online of parent group %1 after child online since local cluster does not have Authority for parent group	Warning	Y	N
50809	HAD	Group %1 is unable to go online on any system in cluster %2	Warning	Y	N
50824	HAD	Command (%1) failed. At least Group Operator privilege required on remote cluster %2	Error	Y	N

