

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

Windows

VCS Library Management Pack



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

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. See the Third-party Legal Notices document for this product, which is available online or included in the base release media.

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

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

Technical Support

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

Symantec's 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_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

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>

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>

Contents

Technical Support	4	
Chapter 1	Deploying the VCS Library Management Pack	9
	About the VCS Library Management Pack	9
	Supported software	10
	About deploying the VCS Library Management Pack	11
	Installing the VCSOpsMgrIntegration service	11
	Importing the VCS Library Management Pack	13
	Installing the Operations Manager agent	14
	Making the Integration service highly available	16
	Configuring agent-managed computers as proxy	17
	Uninstalling the VCSOpsMgrIntegration service	18
Chapter 2	Troubleshooting	19
	About troubleshooting VCS management pack issues	19
	Physical servers are incorrectly discovered as type Ex.Mailbox	19
	Conflict while trying to monitor clusterized standalone instances	20
	Error while re-importing the VCS management packs	20
	VCS virtual server discovery fails	21
	Additional discovery and monitoring of virtual servers for other applications running on cluster nodes	22
	Application instances are not discovered on cluster nodes where the Veritas High Availability engine is not running	22
	Proxy is not set properly for agent-less managed Exchange and SQL virtual servers	22
	Unable to delete Symantec.VCS.Library.mp	23
	VCSOpsMgrIntegration service fails to discover SQL 2012 virtual server after deleting it from the discovery list of Agentless managed computer	23

Deploying the VCS Library Management Pack

This chapter includes the following topics:

- [About the VCS Library Management Pack](#)
- [Supported software](#)
- [About deploying the VCS Library Management Pack](#)
- [Installing the Operations Manager agent](#)
- [Making the Integration service highly available](#)
- [Configuring agent-managed computers as proxy](#)
- [Uninstalling the VCSOpsMgrIntegration service](#)

About the VCS Library Management Pack

The Veritas Cluster Server (VCS) Library Management Pack, *Symantec.VCS.Library.mp*, is required to monitor applications configured under VCS, in a Microsoft System Center Operations Manager (SCOM) monitoring environment.

The VCS Library Management Pack functions as follows:

When you install the Operations Manager agent on physical cluster nodes, the nodes get added to the Agent-Managed group on the management server. When you import the Exchange or SQL management packs on the management server, these management packs discover the clustered Exchange and SQL instances (virtual servers) running on the nodes.

The VCS Library Management Pack invokes the VCSOpsMgrIntegration Service which then connects to the management server and adds the Exchange and SQL virtual servers as agentless managed computers. The service also sets the physical cluster nodes where the Exchange or SQL service groups are online as proxy for the virtual servers. Application monitoring starts as soon as the virtual servers are added as agentless managed objects on the management server.

Consider that you install the Operations Manager agent on cluster node 'N1' and 'N2', having the virtual server name 'V1' for the Exchange Lanman resource. Using the discovery rule the Exchange management pack discover these nodes as "VCS Virtual Server - V1". The VCSOpsMgrIntegration service running on RMS adds the VCS Virtual Server V1 as agent-less managed computers in SCOM server and sets the proxy to 'N1', as V1 is online on N1. Once the virtual server is added as agent-less managed computer in SCOM server, the application monitoring starts.

Note: Apart from monitoring the application, if you wish to monitor the Exchange or SQL service group and its resources, you must import the VCS Management Pack, *Symantec.SFW.HA.mp*.

The VCS Library Management Pack contains the following components:

- Monitor for VCSOpsMgrIntegration Service.
This monitors the state of VCSOpsMgrIntegration service. While the service is running the state is healthy. However, in case of a failure the state is critical.
- Rule to monitor the errors occurred, if any, while processing the data in VCSOpsMgrIntergration Service.
This rule generates an alert in the SCOM server, whenever the VCSOpsMgrIntegration service logs an event in the application event log, with the event id 1.
- A Group, VCS Virtual Server Group, that contains the VCS virtual servers monitored by the SCOM server.
- Two targets, VCS Physical Server, and VCS Virtual Server, representing the physical servers and the VCS virtual servers.

Supported software

The VCS management packs are compatible with the following product versions:

- Microsoft System Center Operations Manager 2007 SP1
- Microsoft System Center Operations Manager 2007 R2
- Microsoft System Center Operations Manager 2012 or later

- Storage Foundation and HA 5.1 for Windows or later
- Veritas Cluster Server 5.1 for Windows or later

For the latest information on the supported software and management pack versions, refer to the following technote:

<http://www.symantec.com/docs/TECH75254>

About deploying the VCS Library Management Pack

This chapter describes how to deploy the VCS Library Management Pack in a Microsoft System Center Operations Manager monitoring environment. Complete the procedures in the given order.

Installing the VCSOpsMgrIntegration service

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

Deploy the VCSOpsMgrIntegration Service only on the Root Management Server (RMS). The service gets installed on the RMS in the “Manual” mode and terminates itself if it fails to connect to the Operations Manager, using the SCOM SDK. The Integration service creates a log file named,

“VCSOpsMgrIntegration.log” at

`%ProgramFiles%\Symantec\MOMUtils\OpsMgr2007` on the RMS node.

Note: The debug logging is disabled by default. You can enable it by creating the registry key "HKLM\Software\Symantec\VCS\OpsMgrIntegration" and setting the DWORD value named 'ServiceLogLevel' with 1 as its value.

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

SQL or Exchange instances (virtual servers) configured with VCS are monitored as agentless managed objects and the cluster nodes on which these virtual servers are configured to run are monitored as agent managed objects.

All the VCS application management packs contain discovery rules to discover the VCS virtual servers for the respective applications. The VCSOpsMgrIntegration

service monitors for the discovery of new VCS virtual servers every 10 minutes and adds them as agentless managed computers to the SCOM Management Server.

When a virtual server comes online, a rule in the VCS library management pack monitors this event and generates an alert that contains information about the virtual server name and the cluster node (physical server) on which the virtual server is online. The Integration service running on the RMS, monitors the Lanman resource, after every 60 seconds and then switches the proxy to the cluster node on which the virtual server is online. The Operations Manager server then starts monitoring the virtual server using the new proxy (node on which the virtual server is online).

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 objects and INST1 is configured as agentless managed object. When INST1 is online on Node1, Operations Manager 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 VCSOpsMgrIntegration Service detects this information from the Lanman agent alert, and switches the proxy to Node2. The Operations Manager server now retrieves INST1 related events from the Node2 event log.

If you modify the Lanman name in your configuration, the new Lanman name as well as the previous Lanman name appears in the discovery list of Agentless managed computer. In this case, manually delete the old Lanman name from the SCOM server. Once deleted, it will not be discovered again.

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

Note: In case you have the earlier version of SCOM pack installed, you must first uninstall the MOMHelper utility and then install the VCSOpsMgrIntegration Service. To uninstall the MOMHelper utility, navigate to the `%programfiles%\symantec\momutils\opsmgr2007` directory on your system and delete the `momhelper.exe` file. Re-navigate to the `%programfiles%\symantec\directory\momutils` location and delete the `opsmgr2007` folder.

To install the VCSOpsMgrIntegration Service

- 1 Insert the product disk into your system's disc drive and navigate to `MOMPacks` directory.

Copy and save the contents to a temporary location on your system.

- 2 From the Operations Manager management server, navigate to the location where you saved the VCSOpsMgrIntegration Service.
- 3 Double-click the **install.bat**. The VCSOpsMgrIntegration Service is installed at the following location on the Operations Manager server:

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

Importing the VCS Library Management Pack

Use the following procedure to import the VCS Library Management Pack, *Symantec.VCS.Library.mp*.

Before you proceed, ensure that the Operations Manager infrastructure is set up and configured correctly. See the Microsoft System Center Operations Manager documentation for more information.

To import the VCS Library Management Pack for SCOM

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
- 2 In the Operations Console, click **Administration**.
- 3 Right-click **Management Packs** to launch the Import Management Packs wizard.
- 4 Click **Add**, and then click **Add from disk**.
- 5 The Select Management Packs to import dialog box appears. Change to the directory that holds the VCS Library Management Pack file, select the management pack **Symantec.VCS.Library.mp** and then click **Open**.

- 6 On the Select Management Packs page, the VCS Library Management Pack that you selected for import is listed. A green check mark indicates that the management pack can be imported. Click **Import**.

A red error icon indicates that the management pack is dependent on one or more management packs that are not in the Import list and are not available in the catalog. To view the missing management packs, click Error in the Status column. To remove the management pack with the error from the Import list, right-click the management pack, and then click **Remove**.
- 7 The Import Management Packs page appears and shows the progress for each management pack. Each management pack is downloaded to a temporary directory, imported to Operations Manager, and then deleted from the temporary directory. If there is a problem at any stage of the import process, select the management pack in the list to view the status details. Click **Close**.

Installing the Operations Manager agent

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

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

To install the Operations Manager agent

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

Making the Integration service highly available

You can make the VCSOpsMgrIntergration service highly available, using the Microsoft Cluster Service (MSCS).

Note: This is an optional task. You can make the Intergration service highly available only if the RMS is clustered using MSCS.

To make the Integration service highly available

- 1 Log on to the computer with an account that is an owner of the RMS cluster group and has administrative rights.
- 2 In Cluster Administrator, right-click the RMS cluster group name.
- 3 From the context menu, select **New > Resource**.
- 4 Using the New Resource Wizard, create a Generic Service Cluster resource for the VCSOpsMgrIntegration service. Enter the following details:
 - Name: VCSOpsMgrIntergration Service
 - Resource type: Generic Service
 - Group: *RMS cluster group name*
- 5 Click **Next**.
- 6 On the Possible Owners panel, ensure that all cluster nodes are listed in the Possible owners box. To add the missing nodes, select the appropriate node from the Available nodes box and click **Add** to add them to the Possible owners box. Click **Next**.

- 7 On the Dependencies panel, select OMSDK, OMCFG and HealthService resources from the Available resources box and click **Add** to include them as Resource dependencies. Click **Next**.
- 8 On the GenericService Parameters panel, in the Service name field, enter **VCSOpsMgrIntegration**.
- 9 Select the Use Network Name for computer name check box, and click **Next**.
- 10 On the Registry Replication panel, click **Finish**.
- 11 Right-click the VCSOpsMgrIntegration service resource and select **Properties**.
- 12 On the Advanced tab, clear the **Affect the group** check box and click **Ok**.

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 server.

After the Operations Manager 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 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 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.

Uninstalling the VCSOpsMgrIntegration service

To uninstall the VCSOpsMgrIntegration service

- 1 Using the command prompt, access the following path:

```
cd %programfiles%\Symantec\MOMUtils\OpsMgr2007
```

- 2 Stop the service. On the command prompt, type the following command.

```
net stop VCSOpsMgrIntegration
```

- 3 Unregister the service, using the following command.

```
VCSOpsMgrIntegration -Uninstall
```

- 4 Access the path `cd %programfiles%\Symantec\MOMUtils` and delete the OpsMgr2007 folder.

Troubleshooting

This chapter includes the following topics:

- [About troubleshooting VCS management pack issues](#)

About troubleshooting VCS management pack issues

This chapter describes the process of recovering from various error conditions that may occur when monitoring applications using the VCS management packs.

Physical servers are incorrectly discovered as type Ex.Mailbox

The VCS Exchange 2007 (converted) management pack incorrectly discovers the physical servers hosting Exchange as being of type Ex.Mailbox.

Perform the following steps to remove the incorrectly discovered instances:

- 1 Create a computer group in Operations Manager and add the physical servers to the group.
- 2 Disable **Microsoft.Exchange.2007.Ex_Common_Class.StateAlertDiscovery** and **Microsoft.Exchange.2007.Ex_Mailbox_Class.StateAlertDiscovery** for the computer group.
- 3 Run the **remove-disabledMonitoringObject** cmdlet from Operations Manager Command Shell to remove the incorrectly discovered instances.

Note: The `remove-disabledMonitoringObject` cmdlet will remove all instances of objects with discovery disabled.

Conflict while trying to monitor clusterized standalone instances

This error may occur in the following scenario. Consider a setup where standalone non-clustered application instances are being monitored by Operations Manager server. Now, if the standalone application instances are made highly available with VCS, and you wish to monitor these clusterized instances with the same Operations Manager server. The Operations Manager server discovery already has the entry of the standalone instance. When you try to re-discover the clusterized virtual instances, it may lead to a conflict.

To fix the problem, do the following:

- 1 Delete the standalone application instance name from the Operations Manager server.
- 2 Configure the application instance under VCS.
- 3 Configure Operations Manager to monitor the clusterized instance.

Error while re-importing the VCS management packs

This issue may occur if you have already deployed the VCS management packs in your Operations Manager monitoring environment and you try to re-import the management packs. The following error message is displayed in the Import Management Packs dialog box:

```
The requested management pack was invalid. See inner exception for details. This version of the management pack is already imported in the database.
```

To re-import the VCS management packs, perform the following steps:

- 1 Check the VCS management pack dependencies.
 - From the Operations Console, click **Administration** and in the Administration pane, click **Management Packs**.
 - In the Management Packs pane, right-click the VCS management pack and then click **Properties**.
 - Click the **Dependencies** tab to view the list of management packs that depend on the selected management pack. Make a note of these management packs.
- 2 Export the dependent management packs that you noted down in step 1 earlier.
 - From the Operations Console, click **Administration** and in the Administration pane, click **Management Packs**.

- In the Management Packs pane, right-click the VCS management pack that you want to export, and then click **Export Management Pack**.
 - In the Save As dialog box, type the path and file name for the Management Pack file, or click **Browse** to save the file to a different directory, and then click **Save**.
 - Repeat this for all the dependent management packs that you noted in step 1.
- 3 Delete the dependent management packs that you noted in step 1.
- From the Operations Console, click **Administration** and in the Administration pane, click **Management Packs**.
 - In the Management Packs pane, right-click the VCS management pack that you want to delete, and then click **Delete**.
 - On the message stating that deleting the Management Pack might affect the scoping of some user roles, click **Yes**.
- 4 Import the management packs that you exported in step 2.
- From the Operations Console, click **Administration**, right-click the Management Packs node and then click **Import Management Packs**.
 - In the Select Management Packs to import dialog box select the management pack that you want to import and then click **Open**.
 - In the Import Management Packs dialog box select the management pack that you selected earlier, and then click **Import**.
- 5 Import the VCS management packs. Refer to step 4 for instructions.

VCS virtual server discovery fails

The Operations Manager server may sometimes fail to discover the virtual servers configured in VCS. This may occur if the VCS virtual servers are not added as agentless managed computers on the management server.

Check the following items:

- Ensure that the VCSOpsMgrIntegration Service is deployed on the management server.
- Ensure that the respective application service group is online in the cluster.
- Make sure that the Lanman agent attributes, ADUpdateRequired and DNSUpdateRequired, are set to True. If they are not, set them to True, and then take the Lanman resource offline and bring it online.

Additional discovery and monitoring of virtual servers for other applications running on cluster nodes

Complete the following steps:

- Override application discoveries to disable them for the VCS Virtual Server Group computer group.
- If you have deployed Operations Manager 2007 Service Pack 1, use `Remove-DisabledMonitoringObject` cmdlet to remove objects for which monitoring is disabled.

Note: `Remove-DisabledMonitoringObject` cmdlet removes all objects for which monitoring is disabled and this includes objects discovered for other management packs as well. Before using the cmdlet, refer to the Operations Manger 2007 documentation for detailed information about its usage.

Application instances are not discovered on cluster nodes where the Veritas High Availability engine is not running

The management pack discovery script uses `VCSOpsMgrIntegration` Service, on cluster nodes to retrieve information from the VCS configuration. If the Veritas High Availability Engine (HAD) is not running on the node, this utility fails and eventually the discovery scripts also fail.

Workaround: Start the Veritas High Availability Engine (HAD) using `hastart` command.

Proxy is not set properly for agent-less managed Exchange and SQL virtual servers

You may find incorrect proxy for virtual servers in case the node on which service group is online gets added to the management server after the virtual server is added as an agentless managed computer.

Workaround:

- 1 Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager management group.
- 2 In the Operations Console, click **Administration > Device Management > Agentless managed**.

- 3 Right-click **Virtual server for proxy is incorrect**.
- 4 Select **Change proxy agent** and then from the displayed list select the Windows computer on which service group is online.

Unable to delete Symantec.VCS.Library.mp

This issue occurs if the Library management pack version has RunAs profile configured and the Management Server Action account does not have permission to connect to operations manager database using SCOM SDK.

Workaround:

- 1 Export the Microsoft.SystemCenter.SecureReferenceOverride mom pack in form of a xml file and save it at some location.
- 2 Delete the Microsoft.SystemCenter.SecureReferenceOverride mom pack.
- 3 Delete the VCS library mom pack.
- 4 Open the exported mp xml file in any xml editor.
- 5 Delete the "Reference" element which refers to "Symantec.VCS.Library" mp.
- 6 Delete the "SecureReferenceOverride" element which overrides "Symantec.VCS.MOMHelperProfile".
- 7 Save the changes and import the modified xml file in MOM.

Note: You must perform these steps only if you want to delete the older versions of Library mp.

VCSOpsMgrIntegration service fails to discover SQL 2012 virtual server after deleting it from the discovery list of Agentless managed computer

The VCSOpsMgrIntegration service monitors for the discovery of new VCS virtual servers every 10 minutes and adds them as agentless managed computers to the SCOM Management Server.

Consider a SQL 2012 virtual server is already added to the SCOM Management Server. If you delete this SQL 2012 virtual server from the discovery list of Agentless managed computer, the VCSOpsMgrIntegration service should discover the SQL 2012 virtual server again after 10 minutes. But the service fails to discover the virtual server.

Workaround:

Restart the VCSOpsMgrIntegration service.

