

Enterprise Vault™ Troubleshooting Operations Manager

8.0 or later

Enterprise Vault™: Troubleshooting Operations Manager

Last updated: 2021-03-23.

Legal Notice

Copyright © 2021 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, Enterprise Vault, Compliance Accelerator, and Discovery Accelerator are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas 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. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

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 Veritas Technologies LLC 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. VERITAS TECHNOLOGIES LLC 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, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on-premises or hosted services. 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.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<https://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/vqa

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://www.veritas.com/docs/100040095>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

evdocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<https://www.veritas.com/community>

Contents

Chapter 1	About this document	6
	About troubleshooting Enterprise Vault Operations Manager	6
Chapter 2	Troubleshooting the installation and configuration of Operations Manager	8
	About troubleshooting the installation and configuration of Operations Manager	8
	Troubleshooting the installation and configuration of Operations Manager	9
	Determining whether Operations Manager is installed and configured successfully	9
	Running the Operations Manager Configuration utility	10
	Configuring Operations Manager manually	11
	Configuring Operations Manager manually: IIS 6	11
	Configuring Operations Manager manually: IIS 7 and later	14
Chapter 3	Troubleshooting accessing Operations Manager	18
	About troubleshooting accessing Operations Manager	18
	Troubleshooting accessing Operations Manager	19
	Authentication failure and access denied message	20
	Parser error: "This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms"	21
	Changing the port for accessing the Monitoring database	22
	Checking the Monitoring Agent and Middle Tier executables	23
Chapter 4	Troubleshooting problems when using Operations Manager	24
	About troubleshooting problems when using Operations Manager	24
	No monitoring data for one or more servers	24
	Vault store performance counters are not shown	25
	Performance counters not shown for a new vault store	25

Checking whether Site monitoring is enabled	26
Fixing problems with performance counters	26

About this document

This chapter includes the following topics:

- [About troubleshooting Enterprise Vault Operations Manager](#)

About troubleshooting Enterprise Vault Operations Manager

This technical note provides troubleshooting information on setting up, accessing, and using Enterprise Vault Operations Manager. It provides help for the following:

- You have a problem when configuring Operations Manager, or you suspect that it may not be configured correctly.
See [“About troubleshooting the installation and configuration of Operations Manager”](#) on page 8.
- You are sure that Operations Manager is configured correctly, but you cannot access it.
See [“About troubleshooting accessing Operations Manager”](#) on page 18.
- You can access Operations Manager successfully but you are having problems with the monitoring data or the reports.
See [“About troubleshooting problems when using Operations Manager”](#) on page 24.

Note: From Enterprise Vault 10.0.3, you can limit the Vault Service account's SQL privileges to increase database security. The Enterprise Vault databases contain a set of roles that enable you to assign to the Vault Service account only those SQL privileges that are required to run Enterprise Vault. However, if you limit the SQL privileges of the Vault Service account for normal daily operations, you may need to grant additional SQL privileges to the account for other tasks that require higher privileges.

For more information on using the SQL Server roles, see the following article on the Support website: <https://www.veritas.com/docs/100038151>.

Troubleshooting the installation and configuration of Operations Manager

This chapter includes the following topics:

- [About troubleshooting the installation and configuration of Operations Manager](#)
- [Troubleshooting the installation and configuration of Operations Manager](#)
- [Determining whether Operations Manager is installed and configured successfully](#)
- [Running the Operations Manager Configuration utility](#)
- [Configuring Operations Manager manually](#)

About troubleshooting the installation and configuration of Operations Manager

This chapter describes how to troubleshoot problems with installing and configuring Enterprise Vault Operations Manager. It assumes that you have attempted to install and configure Operations Manager following the instructions in the *Installing and Configuring* manual.

Note: If you are sure that Operations Manager has been configured successfully, but you are still unable to access it, try troubleshooting access to the installed Operations Manager.

See [“Troubleshooting accessing Operations Manager”](#) on page 19.

Troubleshooting the installation and configuration of Operations Manager

Problem: You had a problem when configuring Operations Manager, or you suspect it did not configure successfully.

Cause: There may have been a configuration failure.

Resolution:

- If you are sure that the configuration has failed, rerun the Operations Manager Configuration utility.
See [“Running the Operations Manager Configuration utility”](#) on page 10.
- Otherwise, verify whether Operations Manager has been set up successfully.
See [“Determining whether Operations Manager is installed and configured successfully”](#) on page 9.

Determining whether Operations Manager is installed and configured successfully

Perform the following procedure to test whether Operations Manager has been installed and configured successfully.

To determine whether Operations Manager is installed and configured successfully

- 1 From the Windows **Start** menu select **Control Panel > Administrative Tools > Internet Information Services Manager**
- 2 Check whether the following are true:
 - The **Application pools** node contains an **EnterpriseVaultMonitoring** application pool.
 - The **Default Web Site** node contains a **MonitoringWebApp** website.

If the application pool and website are present, then Operations Manager is successfully configured. You can continue troubleshooting access to the Operations Manager Configuration utility.

See [“Troubleshooting accessing Operations Manager”](#) on page 19.

Otherwise, Operations Manager is not configured successfully. You need to run or rerun the Operations Manager Configuration utility.

See [“Running the Operations Manager Configuration utility”](#) on page 10.

Running the Operations Manager Configuration utility

You can run or rerun the Operations Manager Configuration utility to configure Operations Manager.

To configure Operations Manager with the Operations Manager Configuration utility

1 Log on to the Enterprise Vault server using the Vault Service account.

2 Click **Start > Programs > Enterprise Vault > Operations Manager Configuration**.

The Operations Manager Configuration utility starts.

3 Provide the details of the monitoring user account you have created for Operations Manager to run under. Enter the Active Directory domain, the user name, and the password for the monitoring user account.

4 Click **Configure** to run the utility.

The utility gives the account the required permissions, and adds the user to the **EnterpriseVaultDirectory** database as the monitoring user.

5 When the utility has finished, click **OK** on the displayed dialog to quit the utility.

Note: If you run this utility to update the details of the monitoring user account, remember to rerun the utility on any other Enterprise Vault server that has Operations Manager installed.

Now try accessing Operations Manager, as described in the *Installing and Configuring* manual, to confirm that it is successfully installed and configured.

If the configuration failed again, you can configure Operations Manager manually.

See [“Configuring Operations Manager manually”](#) on page 11.

Configuring Operations Manager manually

Follow this procedure only if you have attempted to use the Operations Manager Configuration utility and it has failed.

Follow the appropriate instructions depending on the version of Internet Information Services (IIS).

Configuring Operations Manager manually: IIS 6

The procedure is divided into three parts:

- Create the EnterpriseVaultMonitoring application pool in IIS.
- Create the MonitoringWebApp virtual directory.
- Complete the configuration of Operations Manager.

Perform the steps in the order described.

To create the EnterpriseVaultMonitoring application pool

- 1 Confirm that the folder `MonitoringWebApp` is present in the Enterprise Vault installation folder, for example `C:\Program Files\Enterprise Vault`.

If the `MonitoringWebApp` folder is not present, Operations Manager has not been installed. Run the Enterprise Vault installation wizard to install the Operations Manager component, as described in the *Installing and Configuring* manual.
- 2 Open Internet Information Services (IIS) Manager.
- 3 Right-click **Application Pools** in the left pane, and choose **New > Application Pool**.
- 4 In the **Application Pool ID** field, type **EnterpriseVaultMonitoring**.
- 5 Keep **Use default settings for application pool** selected and click **OK** to create the application pool.
- 6 Right-click the **EnterpriseVaultMonitoring** application pool and choose **Properties**.
- 7 On the **Identity** tab, choose **Configurable** and enter the user name and password of the monitoring user.
- 8 Click **OK** complete the changes to the application pool. You are prompted to re-enter the monitoring user password to confirm it. The setting up of the application pool is now complete.

To create the MonitoringWebApp virtual directory

- 1 Expand **Web Sites** in the left pane of IIS Manager, right-click **Default Web Site**, and choose **New > Virtual Directory**.
- 2 On the first page of the **Virtual Directory Creation** wizard, click **Next**.
- 3 When prompted for an alias, type **MonitoringWebApp** and click **Next** to display the **Web Site Content Directory** wizard page.
- 4 To specify the path, browse to the `monitoringwebapp` folder, for example `C:\Program Files\Enterprise Vault\monitoringwebapp`, and click **OK**. Then click **Next** to display the **Virtual Directory Access Permission** wizard page.
- 5 Select the **Read** and **Run scripts (such as ASP)** check boxes and click **Next**.
- 6 Click **Finish** to exit the wizard.
- 7 In the left pane of IIS Manager, right-click **MonitoringWebApp** and choose **Properties**.
- 8 On the **Virtual Directory** tab, in the **Application pool** box, select the **EnterpriseVaultMonitoring** application pool you created earlier.
- 9 On the **Documents** tab, select the **Enable default content page** check box and remove all the pre-existing entries except **default.aspx**.
- 10 On the **Directory security** tab, under **Authentication and access control**, click **Edit**.
- 11 Clear the **Enable anonymous access** check box. Select the **Integrated Windows authentication** check box. Click **OK** to return to the **Properties** dialog.
- 12 In the **ASP.NET** tab, in the **ASP.NET version** box, select **2.0.50727**.
- 13 Click **OK** to close the **Properties** dialog.

To complete the configuration of Operations Manager

- 1 Add the monitoring user to the **IIS_WPG** local group.
- 2 Give read permission to the monitoring user for the following Registry key:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\KVS
\Enterprise Vault
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\Wow6432Node
\KVS
\Enterprise Vault
```

- 3 Give read permission to the monitoring user on the `MonitoringWebApp` folder in the Enterprise Vault installation folder.
- 4 Give read and write permissions to the monitoring user on the `Logs` subfolder of the `MonitoringWebApp` folder.
- 5 Give read, write, and execute permissions to the monitoring user on the folder `C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files`.
- 6 Note the site ID of the computer on which you are configuring Operations Manager. The site ID can be obtained from the **SiteID** value of the following Registry key:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\KVS
\Enterprise Vault
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\Wow6432Node
\KVS
\Enterprise Vault
```

- 7 Open SQL Server Enterprise Manager and browse to the **EnterpriseVaultDirectory** database. Select **Tables** and locate the table **MonitoringSettings**. Right-click **MonitoringSettings** and select **Open Table > Return all rows**.
- 8 Locate the row with the **SiteEntryID** that matches your Site ID.
- 9 Update the **MonitoringUser** column with the domain and user name of the monitoring user, in the format *domain\username*.
- 10 Update the **SiteAddress** column with the address of your Web server. For example, if you have configured **MonitoringWebApp** on the server blackbird, the URL takes the form:

`http://blackbird/monitoringwebapp/default.aspx`
- 11 Close the table.
- 12 Restart the IIS Admin Service.
- 13 Browse to **http://localhost/monitoringwebapp/default.aspx**, and confirm that you can now view Operations Manager.

Configuring Operations Manager manually: IIS 7 and later

The procedure is divided into three parts:

- Create the EnterpriseVaultMonitoring application pool in IIS.
 (For background information on creating application pools with IIS 7, see the following Microsoft article: <https://technet.microsoft.com/library/cc731784.aspx>)
- Create the MonitoringWebApp Web application.
 (For background information on creating Web applications with IIS 7, see the following Microsoft article: <https://technet.microsoft.com/library/cc772042.aspx>)
- Complete the configuration of Operations Manager.

Perform the steps in the order described.

To create the EnterpriseVaultMonitoring application pool

- 1 Confirm that the folder `MonitoringWebApp` is present in the Enterprise Vault installation folder, for example `C:\Program Files\Enterprise Vault`.

 If the `MonitoringWebApp` folder is not present, Operations Manager has not been installed. Run the Enterprise Vault installation wizard to install the Operations Manager component, as described in the *Installing and Configuring* manual.
- 2 Open Internet Information Services (IIS) Manager.

- 3 In the **Connections** pane, expand the server node and click **Application Pools**.
- 4 On the **Application Pools** page, in the **Actions** pane, click **Add Application Pool**.
- 5 In the **Add Application Pool** dialog do as follows:
 - For **Name**, enter **EnterpriseVaultMonitoring**.
 - For **.Net Framework version**, select **.NET Framework v4.0.30319** for Enterprise Vault 12 or **.NET Framework v2.0.50727** for earlier versions of Enterprise Vault.
 - For **Managed pipeline mode**, select **Classic**.
 - Select **Start application pool immediately** to make sure that the application pool starts whenever the WWW service starts.
 - Then click **OK** to add the application pool.
- 6 Right-click the newly created application pool and select **Advanced Settings**.
- 7 In the **Process Model** settings, in **Identity**, specify the user name and password for the monitoring user.
- 8 Click **OK** to close the Advanced Settings dialog.

To create the MonitoringWebApp Web application

- 1 In the **Connections** pane of IIS Manager, expand the **Sites** node.
- 2 Right-click the Default Web Site and click **Add Application**.
- 3 In the **Add Application** dialog, do as follows:
 - In the **Alias** box, enter a value for the application URL, such as **MonitoringWebApp**.
 - For the **Application pool**, click **Select** and select **EnterpriseVaultMonitoring** from the drop-down list, and click **OK**.
 - For **Physical path**, you must specify the physical path of the application's folder. To specify the path, browse to the `monitoringwebapp` folder, for example `C:\Program Files\Enterprise Vault\monitoringwebapp` and click **OK**.
 - Optionally, click **Test Settings** to verify the settings that you specified.
 - Click **OK** to close the dialog.
- 4 With **Features View** selected, open **Default Document** and remove all the pre-existing entries except `default.aspx`.

- 5 Select the MonitoringWebApp Web application and with **Features View** selected, open **Authentication**.
- 6 Enable Windows Authentication and ASP.NET Impersonation, and disable Anonymous Authentication.

To complete the configuration of Operations Manager

- 1 Add the monitoring user to the **IIS_IUSRS** local group.
- 2 Give read permission to the monitoring user for the following Registry key:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\KVS
\Enterprise Vault
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\Wow6432Node
\KVS
\Enterprise Vault
```

- 3 Give read permission to the monitoring user on the `MonitoringWebApp` folder in the Enterprise Vault installation folder.
- 4 Give read and write permissions to the monitoring user on the `Logs` subfolder of the `MonitoringWebApp` folder.
- 5 Give read, write, and execute permissions to the monitoring user on the folder `C:\WINDOWS\Microsoft.NET\Framework\version\Temporary ASP.NET Files` where *version* is v4.0.30319 for Enterprise Vault 12 or v2.0.50727 for earlier versions of Enterprise Vault.

- 6 Note the site ID of the computer on which you are configuring Operations Manager. The site ID can be obtained from the **SiteID** value of the following Registry key:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\KVS
\Enterprise Vault
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\Wow6432Node
\KVS
\Enterprise Vault
```

- 7 Open SQL Server Enterprise Manager and browse to the **EnterpriseVaultDirectory** database. Select **Tables** and locate the table **MonitoringSettings**. Right-click **MonitoringSettings** and select **Open Table > Return all rows**.
- 8 Locate the row with the **SiteEntryID** that matches your Site ID.
- 9 Update the **MonitoringUser** column with the domain and user name of the monitoring user, in the format *domain\username*.
- 10 Update the **SiteAddress** column with the address of your Web server. For example, if you have configured **MonitoringWebApp** on the server blackbird, the URL takes the form:

`http://blackbird/monitoringwebapp/default.aspx`
- 11 Close the table.
- 12 Restart the IIS Admin Service.
- 13 Browse to **http://localhost/monitoringwebapp/default.aspx**, and confirm that you can now view Operations Manager.

Troubleshooting accessing Operations Manager

This chapter includes the following topics:

- [About troubleshooting accessing Operations Manager](#)
- [Troubleshooting accessing Operations Manager](#)
- [Authentication failure and access denied message](#)
- [Parser error: “This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms”](#)
- [Changing the port for accessing the Monitoring database](#)
- [Checking the Monitoring Agent and Middle Tier executables](#)

About troubleshooting accessing Operations Manager

This chapter describes how to troubleshoot problems with accessing Enterprise Vault Operations Manager. It assumes that you have confirmed that Operations Manager has installed and configured successfully, as described in the previous chapter.

Note: If you can successfully access the Operations Manager user interface but you are having problems with the displayed data, troubleshoot the using of Operations Manager.

See [“About troubleshooting problems when using Operations Manager”](#) on page 24.

Troubleshooting accessing Operations Manager

Problem: You have verified that Operations Manager is successfully installed and configured, but you cannot access it.

Resolution: Use the following procedure to identify and resolve the problem:

To troubleshoot accessing Operations Manager

- 1 If, when you attempt to access Operations Manager, you are asked to authenticate three times and receive an “access denied” message, refer to the Microsoft support article in the following section

See [“Authentication failure and access denied message”](#) on page 20.

- 2 If you enable or disable the Windows policy setting for FIPS-compliant algorithms on a computer on which Operations Manager is configured, you must then re-run the Operations Manager Configuration utility. Otherwise when you subsequently run Operations Manager, the Web browser displays a parser error message stating that the implementation is not part of the Windows Platform FIPS validated cryptographic algorithms.

See [“Parser error: “This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms””](#) on page 21.

- 3 Check whether port 8071 is used by a program other than the Enterprise Vault `MonitoringMiddleTier.exe` program. If another program uses this port, the Operations Manager Web application will not appear. You can check whether a port is in use by running the following command from a command prompt window:

```
netstat -b
```

If required, you can change the port that `MonitoringMiddleTier.exe` uses.

See [“Changing the port for accessing the Monitoring database”](#) on page 22.

- 4 Check whether the Monitoring Agent and Monitoring Middle Tier executables are running. See [“Checking the Monitoring Agent and Middle Tier executables”](#) on page 23.
- 5 Confirm that the prerequisites for Operations Manager are satisfied, as described in the *Installing and Configuring* manual.
- 6 If you are running Operations Manager on a 64-bit computer, make sure that you have switched to the 32-bit version of ASP.NET, as described in the *Installing and Configuring* manual.
- 7 Confirm that IIS is not locked down.

- 8 Check that the IIS_WPG group (for IIS 6) or the IIS_IUSRS group (IIS 7) has read/write access onto the folder <EVInstall_path>\MonitoringWebApp\Logs, where <EVInstall_path> is the location of the EV installation folder, for example C:\Program Files\Enterprise Vault.
- 9 Check that the identity for the **EnterpriseVaultMonitoring** application pool is set to the MonitoringUser Windows user account you created for Operations Manager to use.
- 10 Ensure that the MonitoringUser account is a member of the following group in Active Directory:
 - For IIS 6, the IIS_WPG group
 - For IIS 7, the IIS_IUSRS group
- 11 This step applies to IIS 6 only. For IIS 7, go to the next step.

From the Windows Start menu select **Control Panel > Administrative Tools > Internet Information Services Manager** and check that the properties of the **MonitoringWebApp** website are as follows:

- The ASP.NET version on the ASP.NET property tab is set to **2.***
- The application pool is set to **EnterpriseVaultMonitoring**.
- For authentication, Integrated Windows authentication is selected.

- 12 This step applies to IIS 7 only.

From the Windows Start menu select **Control Panel > Administrative Tools > Internet Information Services Manager**, and do as follows:

- Check in the Advanced Settings of the **MonitoringWebApp** website that the application pool is set to **EnterpriseVaultMonitoring**.
- Check in the Basic Settings of the application pool **EnterpriseVaultMonitoring**, that the .NET Framework version is set to **v4.*** for Enterprise Vault 12 or **v2.*** for earlier versions of Enterprise Vault.
- Open the Authentication page in the Features View of the **MonitoringWebApp** site. Make sure that the status of Windows authentication is **Enabled**

Authentication failure and access denied message

Problem: When you attempt to access Operations Manager you are asked to authenticate three times and then you receive an “access denied” message.

Parser error: “This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms”

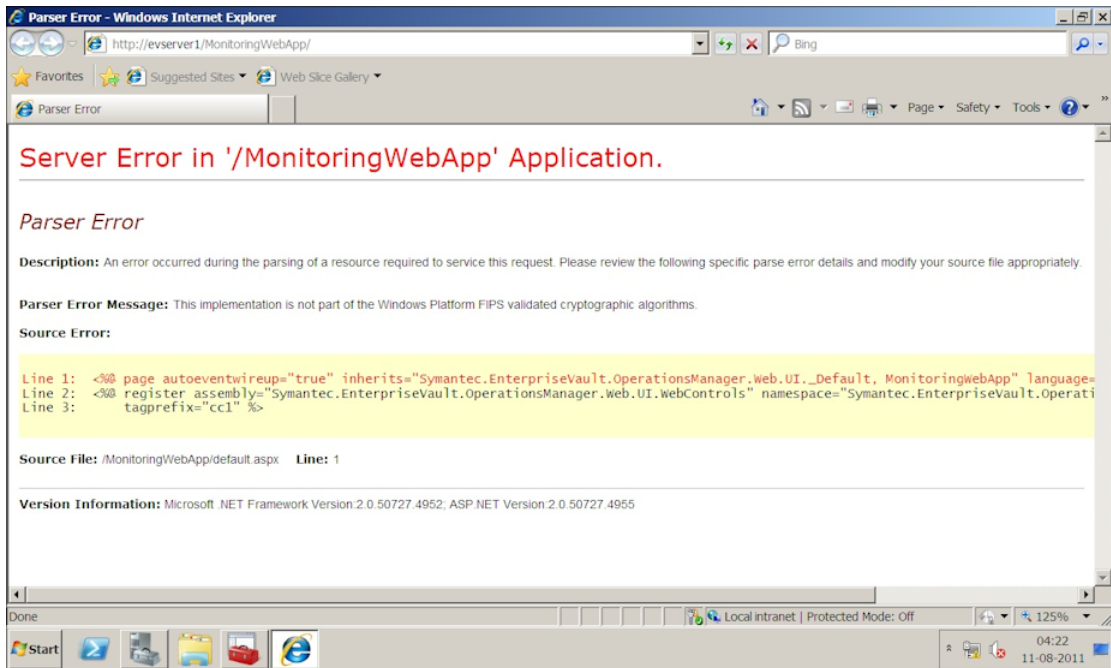
Cause: This is a known authentication problem which is documented in the Microsoft support article *Authentication may fail with “401.3” Error if Web site’s “Host Header” differs from server’s NetBIOS name* (<http://support.microsoft.com/?id=294382>).

Resolution: Follow the instructions in the support article to run the following command on the Enterprise Vault server on which Operations Manager is installed:

```
cscript adsutil.vbs set w3svc/NTAuthenticationProviders "NTLM"
```

Parser error: “This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms”

Problem: When you attempt to access Operations Manager, the browser displays a parser error similar to the following:



The parser error message states that “This implementation is not part of the Windows Platform FIPS validated cryptographic system.”

Cause: The browser displays this error if you attempt to access Operations Manager after you enable or disable the following Windows security setting, either in the Windows Local Security policy, or as part of the Group Policy:

System cryptography: use FIPS compliant algorithms for encryption, hashing, and signing

Resolution: After you enable or disable the Windows policy setting for FIPS-compliant algorithms on a computer on which Operations Manager is configured, you must rerun the Operations Manager Configuration utility.

See [“Running the Operations Manager Configuration utility”](#) on page 10.

Changing the port for accessing the Monitoring database

Operations Manager accesses the Monitoring database through the `MonitoringMiddleTier.exe` process, which is spawned by the Enterprise Vault Admin service. By default, Operations Manager and `MonitoringMiddleTier.exe` communicate with each other using port 8071. If port 8071 is used by another program, you need to change the port that is used by Operations Manager and `MonitoringMiddleTier.exe`.

To change the communications port

- 1 Navigate to the top-level Enterprise Vault installation folder, for example `C:\Program Files\Enterprise Vault`.
- 2 Open the `MonitoringMiddleTier.exe.config` configuration file with a simple text editor such as Notepad.
- 3 Change the port number that is specified in the following line of the file to an available port number of your choice:

```
<channel ref="tcp" port="8071" >
```

- 4 Save and close the file.
- 5 Navigate to the `MonitoringWebApp` subfolder, for example `C:\Program Files\Enterprise Vault\MonitoringWebApp`.
- 6 Open the `web.config` configuration file with a simple text editor such as Notepad.
- 7 Change the port number that is specified in the following line of the file to an available port number of your choice:

```
<add key="OMMiddleTierPort" value="8071"/>
```

- 8 Save and close the file.
- 9 Restart the Enterprise Vault Admin service.
- 10 Restart the IIS Admin service.

Checking the Monitoring Agent and Middle Tier executables

The Enterprise Vault Admin service attempts to spawn the Monitoring Agent and Monitoring Middle Tier executables up to three times. If the Admin service fails to start these executables you need to investigate why.

To check the Monitoring Agent and Middle Tier executables

- 1 Right-click an empty space on the Windows task bar, and then click **Task Manager**.
- 2 Click Task Manager's **Properties** tab.
- 3 Check whether `MonitoringAgent.exe` and `MonitoringMiddleTier.exe` are running. If they are, continue with the next diagnostic step to troubleshoot accessing an installed Operations Manager. See [“Troubleshooting accessing Operations Manager”](#) on page 19. If you cannot see these programs listed in Task Manager, continue with the following.
- 4 Examine the application event logs for entries logged by the .NET runtime process around the time that the Admin service started, for indications as to why `MonitoringAgent.exe` and `MonitoringMiddleTier.exe` did not start.
- 5 If you cannot find any entries in the event logs, run `DTrace` on `adminservice.exe`, restart the Admin service, and then search the `DTrace` logs for entries from the function `StartProcessesInList()`. This gives you a specific Windows error code that indicates why the launch of the executables failed.

For details of how to use `DTrace`, see the Enterprise Vault *Utilities* manual.

After rectifying the problem, restart the Admin service and then repeat steps 1 to 3 to confirm that both executables are now running.

Troubleshooting problems when using Operations Manager

This chapter includes the following topics:

- [About troubleshooting problems when using Operations Manager](#)
- [No monitoring data for one or more servers](#)
- [Vault store performance counters are not shown](#)

About troubleshooting problems when using Operations Manager

This chapter describes how to troubleshoot specific problems when using Operations Manager.

No monitoring data for one or more servers

Problem: You can successfully access the Operations Manager user interface, but you see no monitoring data at all for one or more of the Enterprise Vault servers or Exchange journal mailboxes.

Cause: This is likely to be due to a problem with the Monitoring agents.

Resolution: For more details, refer to the *Troubleshooting the Monitoring agents* chapter of the following technical note on the Support website:

<https://www.veritas.com/docs/100018087>

Vault store performance counters are not shown

Problem: Operations Manager does not display the performance counter instances for some or all vault stores.

Cause: There are a number of possible causes:

- If the problem is specific to a newly created vault store, the vault store monitoring start time may not yet have been reached.
 See [“Performance counters not shown for a new vault store”](#) on page 25.
- Site monitoring may not be enabled.
 See [“Checking whether Site monitoring is enabled”](#) on page 26.
- There may be an issue with the performance counters themselves.
 See [“Fixing problems with performance counters”](#) on page 26.

Performance counters not shown for a new vault store

Problem: Operations Manager does not display vault store performance counter values for a new vault store.

Cause: Operations Manager does not begin displaying performance counter values until the monitoring start time has been reached. The monitoring start time and monitoring frequency for the vault store performance counters is set on the **Monitoring** tab of the **Site Properties** dialog in the Enterprise Vault Administration Console. Monitoring begins at the “Start At” time (default 09:00) and occurs at the specified “Frequency” setting (default 1 day).

This means that, for example, if you create a vault store after the monitoring “Start At” time on a given day, and the Frequency is set to 1 day, the server does not monitor the new vault store performance counters until the monitoring “Start At” time on the following day.

Operations Manager displays the data for the new vault store following the first time the Enterprise Vault Monitoring agent monitors the server after the “Start At” time has passed.

Resolution: As a workaround for this known issue, change the performance counter monitoring “Start At” time or Frequency on the **Monitoring** tab of the **Site Properties** dialog so that the Vault store performance counters are monitored immediately. Ensure that the **Enable monitoring for this site** check box is selected, and then restart the Enterprise Vault Admin service. The data for the new Vault store should appear in Operations Manager within a few minutes.

Note that once monitoring has started, the vault store performance counter values get updated at the Operations Manager monitoring frequency, regardless of the frequency set on the Administration Console’s site Monitoring tab. However, any

threshold level breaches generate event logs at the site monitoring frequency. For example, suppose that the site monitoring frequency is set to 1 day and starts at 09:00, and the Operations Manager monitoring frequency is 15 minutes. In this case, the performance counters are sampled every 15 minutes and their updated values are displayed by Operations Manager. However, any threshold breaches as specified by the threshold value in the Site Monitoring dialog in Administration Console are reported in the event log at 09:00 each day.

Checking whether Site monitoring is enabled

Problem: Operations Manager does not display any vault store related performance counters.

Cause: A possible cause is that site monitoring is not enabled in the Enterprise Vault Administration Console. If site monitoring is not enabled, Operations Manager does not sample or display vault store related performance counters.

Resolution: To ensure that Site Monitoring is enabled, right-click the site node in the Enterprise Vault Administration Console and select **Properties**. Then, on the **Properties** dialog, select the **Monitoring** tab. Ensure that the **Enable monitoring for this site** check box is selected.

Fixing problems with performance counters

Problem: Operations Manager does not display any vault store related performance counters.

Cause: If the **Enterprise Vault::Monitoring** performance object is not visible in `perfmon`, then assuming that the Admin Service is started and the Monitoring agent is running, there may be an issue with performance counters on the computer.

Resolution: Use the following procedure to troubleshoot the performance counter issues.

To troubleshoot performance counter issues

- 1 Run the Windows **Services** snap-in and confirm that the Enterprise Vault Admin Service is started.
- 2 Confirm that the Monitoring Agent executable is running. See [“Checking the Monitoring Agent and Middle Tier executables”](#) on page 23.
- 3 Run the Windows Performance Monitor `perfmon`.
- 4 Select **System Monitor** in the Performance Monitor’s left pane, and then type **Ctrl+i** to display the **Add Counters** dialog.

- 5 Check whether the **Enterprise Vault::Monitoring** object is listed in the **Performance object** drop-down box.
- 6 If the **Enterprise Vault::Monitoring** object is not listed, check the Windows Event log for errors relating to performance counters from the .NET framework library and ASP.NET. If you see such errors, follow the instructions in the Microsoft knowledge base article <http://support.microsoft.com/kb/300956> to run `lodctr` with the `/R` option to rebuild the performance counters.