Enterprise Vault™ Deployment Scanner

12.3

VERITAS™

Enterprise Vault™: Deployment Scanner

Last updated: 2018-03-29.

Legal Notice

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

About this guide

This chapter includes the following topics:

- Introducing this guide

- Where to get more information about Enterprise Vault

Introducing this guide

Before you install or upgrade Enterprise Vault, you should run Deployment Scanner to report on the configuration of the computer, including any issues that may prevent Enterprise Vault from running on it.

This guide contains the following information:

- Descriptions of the tests that Deployment Scanner runs on your computer

- How to install Deployment Scanner

- How to run Deployment Scanner

- Troubleshooting information

- How to export a report about your environment

Where to get more information about Enterprise Vault

Table 1-1 lists the documentation that accompanies Enterprise Vault. This documentation is also available in PDF and HTML format in the Veritas Documentation Library.

Table 1-1   Enterprise Vault documentation set

Document	Comments
Veritas Enterprise Vault Documentation Library	Includes all the following documents in Windows Help (`.chm`) format so that you can search across them all. It also includes links to the guides in Acrobat (`.pdf`) format.
	You can access the library in several ways, including the following:
	■ In Windows Explorer, browse to the `Documentation\`*`language`*`\Administration Guides` subfolder of the Enterprise Vault installation folder, and then open the `EV_Help.chm` file. ■ On the **Help** menu in the Administration Console, click **Help on Enterprise Vault**.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the required software and settings before you install Enterprise Vault.
Installing and Configuring	Provides detailed information on setting up Enterprise Vault.
Upgrade Instructions	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up File System Archiving	Describes how to archive files that are held on network file servers.
Setting up IMAP	Describes how to configure IMAP client access to Exchange archives and Internet Mail archives.
Setting up SharePoint Server Archiving	Describes how to archive documents from Microsoft SharePoint servers.
Setting up Skype for Business Archiving	Describes how to archive Skype for Business sessions.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.

Table 1-1 Enterprise Vault documentation set *(continued)*

Document	Comments
Classification using the Microsoft File Classification Infrastructure	Describes how to use the classification engine that is built into recent Windows Server editions to classify all new and existing archived content.
Classification using the Veritas Information Classifier	Describes how to use the Veritas Information Classifier to evaluate all new and archived content against a comprehensive set of industry-standard classification policies. If you are new to classification with Enterprise Vault, we recommend that you use the Veritas Information Classifier rather than the older and less intuitive File Classification Infrastructure engine.
Administrator's Guide	Describes how to perform day-to-day administration procedures.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
Auditing	Describes how to collect auditing information for events on Enterprise Vault servers.
Backup and Recovery	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
Reporting	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
NSF Migration	Describes how to import content from Domino and Notes NSF files into Enterprise Vault archives.
PST Migration	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
Utilities	Describes Enterprise Vault tools and utilities.
Registry Values	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.

Table 1-1   Enterprise Vault documentation set *(continued)*

Document	Comments
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

For the latest information on supported devices and versions of software, see the Enterprise Vault Compatibility Charts.

Enterprise Vault training modules

Veritas Education Services provides comprehensive training for Enterprise Vault, from basic administration to advanced topics and troubleshooting. Training is available in a variety of formats, including classroom-based and virtual training.

For more information on Enterprise Vault training, curriculum paths, and certification options, see https://www.veritas.com/services/education-services.

Veritas Enterprise Vault Deployment Scanner

This chapter includes the following topics:

- About Enterprise Vault Deployment Scanner

- Installing Enterprise Vault Deployment Scanner

- Running Enterprise Vault Deployment Scanner

- Troubleshooting Enterprise Vault Deployment Scanner

About Enterprise Vault Deployment Scanner

Enterprise Vault Deployment Scanner reviews the configuration of a computer and reports on any issues that may stop Enterprise Vault from running on it.

Table 2-1 describes the tests that Enterprise Vault Deployment Scanner performs.

Table 2-1 Enterprise Vault Deployment Scanner tests

Test name	Description
.NET Framework	Checks that the installed version of .NET Framework is compatible with Enterprise Vault.
ASP.NET	Checks that ASP.NET has been installed.
Active Server Pages (ASP)	Checks that Active Server Pages have been installed.
AntiVirus Test	Warns that any antivirus software that is installed on the Enterprise Vault server must be correctly configured to work with Enterprise Vault.

Table 2-1　　　　Enterprise Vault Deployment Scanner tests *(continued)*

Test name	Description
Classification Requirements	Checks that the server meets the requirements for Enterprise Vault classification using the File Server Resource Manager in Windows: ■ The File Server Resource Manager service must be installed. ■ The Microsoft Data Classification Toolkit is required to deploy FSRM classification rules from this server to other Enterprise Vault servers. These components are not required for classification using the Veritas Information Classifier.
DCOM	Checks that DCOM support is enabled. Checks that firewalls that are protecting network access to the Enterprise Vault server are configured to allow access through the following ports: ■ RPC Endpoint Mapper Port (TCP port 135) ■ RPC Dynamic Ports (TCP port range 1024 through 65535)
Directory Database Upgrade	Checks that there is enough disk space on the Directory database computer to upgrade the database for the latest version of Enterprise Vault.
Disk Storage	Reports on the total space and available space for all fixed disks and indicates which one is the system drive.
EMC Centera Connectivity	Checks the connectivity to Centera access nodes.
Enterprise Vault Search Requirements	Checks that the server meets the requirements to host the Enterprise Vault Search facility.
Enterprise Vault Server Version	Reports on the installed version of Enterprise Vault, if present.
Exchange Server Permissions	Checks that the Vault Service account has sufficient permissions against Active Directory.
Exchange Server Version	Reports on the installed version of Microsoft Exchange Server.

Table 2-1   Enterprise Vault Deployment Scanner tests *(continued)*

Test name	Description
FSA Clustering	Checks that the version of the clustering software (Veritas Cluster Server or Windows Server Failover Clustering) on the file server is compatible with Enterprise Vault.
FSA Metadata Migration	Checks for any File System Archiving (FSA) Reporting data that requires upgrading before you can upgrade to the latest version of Enterprise Vault.
File Server .NET Framework Version	Checks that the version of the .NET Framework on the file server is compatible with Enterprise Vault.
File Server .NET Framework WOW64 feature	Checks that the required WOW64 features are enabled on the file server.
File Server Permissions	Checks that the Vault Service account has the correct privileges on the file server.
File Share Permissions	Checks that the Vault Service account has the correct privileges on the file share.
IIS	Checks that the installed version of IIS is compatible with Enterprise Vault. Checks that the IIS components that Enterprise Vault requires are installed. Checks that ASP server-side and client-side script debugging are not set for the web service, web server, or Enterprise Vault virtual directory. Checks that Windows Server Update Services role is not installed.
IMAP Ports	Warns that you must open appropriate ports on the Enterprise Vault server if you want to provide IMAP access to users' archives.
Indexing Requirements	Checks that the installation path for Enterprise Vault does not include non-ASCII characters. Checks that the Net.TCP Port sharing service, World Wide Web Publishing service, and Web Server (IIS) CGI feature are enabled. If Veritas NetBackup or Veritas Backup Exec is detected, checks that the installed version is compatible with Enterprise Vault.

Table 2-1   Enterprise Vault Deployment Scanner tests *(continued)*

Test name	Description
Internet Explorer	Checks that the installed version of Internet Explorer is compatible with Enterprise Vault.
Language Setting	Checks for any issues with the Windows language settings on the Enterprise Vault server.
License Check	Checks for a valid Veritas license.
Lotus Domino Server Version	Reports on the installed version of Domino Server.
Lotus Notes	Checks that the Notes client has been installed.
MMC Version	Reports on the installed version of Microsoft Management Console (MMC).
MSDB Permissions	Warns that if the Vault Service account does not have the systems administrator role on all SQL Server instances that host Enterprise Vault databases, then the Vault Service account requires additional rights on the msdb system database.
MSMQ Configuration	Checks that Microsoft Message Queuing (MSMQ) has been installed without Active Directory integration, and that all the storage directories are on non-system drives.
MSMQ Permissions	Checks that the Vault Service account has sufficient permissions to create the queues that Enterprise Vault uses.
Memory	Reports on the total amount and available amount of physical memory and virtual memory. Warns if the page file is not system managed and is smaller than the size of the physical memory.
Microsoft Cluster Server (MSCS)	Checks that the installed version of Windows Server Failover Clustering is compatible with Enterprise Vault. (Windows Server Failover Clustering was formerly known as *Microsoft Cluster Server*, or *MSCS*.)
Microsoft Updates	Lists all the installed Microsoft updates.
OCR Conversion	Checks that the Windows feature, Windows TIFF IFilter, is installed. This feature is required for Optical Character Recognition (OCR) conversion support.

Table 2-1   Enterprise Vault Deployment Scanner tests *(continued)*

Test name	Description
Operating System	Checks that Enterprise Vault supports the installed version of the operating system and associated service packs.
	The test also checks that you have installed the Desktop Experience feature on the computer. This feature is required for optimum performance of the Enterprise Vault Administration Console.
Outlook Profile	Checks that a valid Microsoft Outlook profile has been created.
Outlook Version	Reports on the version of Microsoft Outlook.
PowerShell	Checks that a suitable version of Windows PowerShell is installed.
Processor	Reports processor information.
Registry Check: AttachmentMax	Reports on whether the AttachmentMax registry value is set according to best practice.
Registry Check: DisableLoopbackCheck	Reports on whether the DisableLoopbackCheck registry key has been set.
Registry Check: DisableStrictNameChecking	Reports on whether the DisableStrictNameChecking registry key has been set.
Registry Check: RecipientMax	Reports on whether the RecipientMax registry value is set according to best practice.
SQL Collation	Reports any mixed collation in the Enterprise Vault directory databases and vault stores.
SQL Database Compatibility	Reports on whether all Enterprise Vault databases are running in a supported compatibility mode.
SQL Server Connectivity	Checks that the SQL Server supports network connections over the TCP/IP and named pipe protocols.
SQL Server Permissions	Checks that the Vault Service account has adequate SQL Server permissions.
SQL Server Reporting Services	Reports on whether a supported version of SQL Server Reporting Services is present.

Table 2-1   Enterprise Vault Deployment Scanner tests *(continued)*

Test name	Description
SQL Server Version	Reports on the installed version of SQL Server, and warns if it is below the minimum required for Compliance Accelerator and Discovery Accelerator.
SharePoint	Checks that SharePoint is installed on the target system. If SharePoint 2013 or later is installed, checks that the Claim to Windows Token Service (C2WTS) is configured and running. On the target server, checks that DCOM port 135 is open in the firewall for incoming connections.
TEMP Folder Security	Checks that there is no unauthorized access to the TEMP folder.
VCS Authentication Client Binaries	Checks for the presence of these binaries, which are needed on the Enterprise Vault server if you want to configure FSA services for high availability on a VCS-clustered file server.
VERITAS Cluster Server Version	Checks that the installed version of Veritas Cluster Server (VCS) is compatible with Enterprise Vault.
VMware server	Checks whether the server is virtual or physical, and provides a link to best practices when deploying Enterprise Vault in a VMware virtual environment.
Vault Service Account	Checks that the Vault Service account is a member of the local Administrators' group.

Installing Enterprise Vault Deployment Scanner

Deployment Scanner is automatically installed in the Enterprise Vault program folder. The installation package, `Veritas Enterprise Vault Deployment Scanner.msi`, is also available in the Enterprise Vault media in the folder `Veritas Enterprise Vault\Deployment Scanner`.

If you do not have Enterprise Vault installed, or access to the Enterprise Vault media, a separate Deployment Scanner installable is available to check the readiness of your system for Enterprise Vault. To obtain the installable, contact Veritas Technical Support.

To install Enterprise Vault Deployment Scanner separately

1   Copy the supplied `.msi` file to the computer on which you want to run Enterprise
Vault Deployment Scanner.

You should run Deployment Scanner on the computer on which you intend to
install the Enterprise Vault services.

2   In Windows Explorer, double-click the `.msi` file.

3   Follow the on-screen instructions.

Running Enterprise Vault Deployment Scanner

Enterprise Vault Deployment Scanner has a wizard-like interface that guides you
through the test process.

You are given the option of running Deployment Scanner when you start the
Enterprise Vault installation program. Alternatively, you can run it separately at any
time.

Note: Before you run Deployment Scanner, add the Vault Service account to the
Administrators group on all the systems that it will scan.

To run Enterprise Vault Deployment Scanner

1   Log on using the Vault Service account.

2   Use one of the following methods to start Deployment Scanner:

■   In Windows, click the **Deployment Scanner** shortcut.

■   In the left pane of the Vault Administration Console, click your vault site.
Then, on the **Tools** menu, ensure that **Advanced Features** is selected.
Finally, in the left pane, right-click your Enterprise Vault server and then
click **Deployment Scanner**.

■   Locate and double-click the Deployment Scanner executable,
`Deployment_Scanner.exe`. You can run the executable on the local
computer or on a remote computer, as required. After Enterprise Vault is
installed, the file is also available in the Enterprise Vault program folder.

3   In the Welcome page, select **Do not set configuration options for
Deployment Scanner** if you have previously run Deployment Scanner and
want to rerun it without entering the configuration options again.

4 Click **Next** and then, if you selected **Do not set configuration options for Deployment Scanner**, go to step 6. Otherwise, complete the fields in the two Server Configuration pages.

Microsoft SQL Server(s)	Identifies the computers on which you have installed SQL Server. Enterprise Vault uses SQL Server to store configuration data and information about the archives.
Microsoft Exchange Server(s)	Identifies the Microsoft Exchange servers from which you want to archive the items in user mailboxes, journal mailboxes, or public folders.
Microsoft SharePoint Server(s)	Specifies the addresses of the Microsoft SharePoint servers that hold the documents you want to archive.
File Server(s)	Identifies the file servers that contain files for archiving.
File Share(s)	Specifies the paths to the network shares that contain files for archiving.
EMC Centera Access Node(s)	Specifies the IP addresses of access nodes in a Centera cluster.

In each case, you can add a new item by typing its name or address and then clicking **Add**. To remove an item from a list, click it and then click **Remove**.

5 When you have set all the options, click **Next** to proceed with the tests.

6 Wait a few moments for the utility to perform the tests and display the results.

7 Click the blue links to display more information on each test result. As well as displaying the test results on-screen, Enterprise Vault Deployment Scanner saves the report to an HTML file in the `Reports` subfolder. The name of the report file identifies the date and time at which you created it.

8 Click **Finish** to exit Enterprise Vault Deployment Scanner.

Troubleshooting Enterprise Vault Deployment Scanner

Table 2-2 lists some error messages that you may see when you run Enterprise Vault Deployment Scanner.

Table 2-2   Enterprise Vault Deployment Scanner error messages

Message	Possible cause
Could not load configuration file! The configuration data for this product is corrupt. Or: Could not load configuration file! The system cannot find the file specified.	The `PreReqConfig.xml` file may be missing or corrupt. This file must be in the folder where you have installed Enterprise Vault Deployment Scanner.
Could not save configuration file! Access is denied.	The `PreReqConfig.xml` file may be read-only.
Could not scan computer! Access is denied.	The `Reports` subfolder may be read-only.
Could not scan computer! Class not registered.	The `PreReqScan.dll` file may not be registered. Open a Command Prompt window and type the following to register the file: `regsvr32 path\PreReqScan.dll`
Could not scan computer! The data is invalid.	The `PreReqStyle.xsl` file may be absent. This file must be in the folder where you have installed Enterprise Vault Deployment Scanner.

Exporting information about your environment using Deployment Scanner

If you are an existing Enterprise Vault user who is experiencing problems because of environmental factors, you can launch Veritas Quick Assist from Deployment Scanner. Veritas Quick Assist collects and exports configuration information in a form that Veritas Technical Support can analyze.

Note: If Veritas Quick Assist has Internet access, it automatically checks for and downloads a newer version. For more information, see the following article on the Veritas Support website:

https://www.veritas.com/docs/100014202

To export information about your environment using Enterprise Vault Deployment Scanner

◆   On the Welcome page of Deployment Scanner, select **Gather information through Veritas Quick Assist** and then click **Finish**.

Deployment Scanner launches Veritas Quick Assist.