

Enterprise Vault™ Auditing

12.3

Enterprise Vault™: Auditing

Last updated: 2018-02-25.

Legal Notice

Copyright © 2018 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
500 E Middlefield Road
Mountain View, CA 94043

<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 guide	6
	Introducing this guide	6
	Where to get more information about Enterprise Vault	6
	Enterprise Vault training modules	9
Chapter 2	Introducing Enterprise Vault auditing	10
	About Enterprise Vault auditing	10
Chapter 3	Setting up auditing	12
	Setting up auditing	12
	Creating the audit database	13
	Configuring audit categories	14
	Starting or stopping auditing	17
	Tuning auditing	18
	Moving the auditing database	18
Chapter 4	Viewing the audit database entries	19
	About viewing the audit database entries	19
	Viewing the audit database entries using Audit Viewer	19
	Using Audit Viewer to run a report on audit data	19
	Copying the search results from Audit Viewer	21
	Changing Audit Viewer settings	21
	Viewing the audit database entries using SQL queries	21
	Retrieving audited changes to archive permissions in a user-friendly format	23
Chapter 5	Auditing for data protection compliance	25
	Auditing general delete operations	25
	Example query search for general item delete audit entries	27
	Auditing privileged delete operations	29
	Example query search for privileged delete audit entries	29

Appendix A	Format of audit database entries	31
	The format of audit database entries	31

About this guide

This chapter includes the following topics:

- [Introducing this guide](#)
- [Where to get more information about Enterprise Vault](#)

Introducing this guide

This guide describes how to set up Enterprise Vault auditing.

Enterprise Vault auditing records activity in a number of different categories. You select the categories in which you want to record activity, and Enterprise Vault stores the recorded information in the Enterprise Vault audit database. You can then view the audit database entries using SQL queries, or use the Audit Viewer utility.

Auditing is an important tool for providing evidence of compliance with data protection regulations. For example, you can use Enterprise Vault classification to mark personally identifiable information (PII), and then enable auditing to record when the PII is deleted.

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	<p>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.</p> <p>You can access the library in several ways, including the following:</p> <ul style="list-style-type: none"> ■ 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.
<i>Introduction and Planning</i>	Provides an overview of Enterprise Vault functionality.
<i>Deployment Scanner</i>	Describes how to check the required software and settings before you install Enterprise Vault.
<i>Installing and Configuring</i>	Provides detailed information on setting up Enterprise Vault.
<i>Upgrade Instructions</i>	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
<i>Setting up Domino Server Archiving</i>	Describes how to archive items from Domino mail files and journal databases.
<i>Setting up Exchange Server Archiving</i>	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
<i>Setting up File System Archiving</i>	Describes how to archive files that are held on network file servers.
<i>Setting up IMAP</i>	Describes how to configure IMAP client access to Exchange archives and Internet Mail archives.
<i>Setting up SharePoint Server Archiving</i>	Describes how to archive documents from Microsoft SharePoint servers.
<i>Setting up Skype for Business Archiving</i>	Describes how to archive Skype for Business sessions.
<i>Setting up SMTP Archiving</i>	Describes how to archive SMTP messages from other messaging servers.

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

Document	Comments
<i>Classification using the Microsoft File Classification Infrastructure</i>	Describes how to use the classification engine that is built into recent Windows Server editions to classify all new and existing archived content.
<i>Classification using the Veritas Information Classifier</i>	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.
<i>Administrator's Guide</i>	Describes how to perform day-to-day administration procedures.
<i>PowerShell Cmdlets</i>	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
<i>Auditing</i>	Describes how to collect auditing information for events on Enterprise Vault servers.
<i>Backup and Recovery</i>	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.
<i>Reporting</i>	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.
<i>NSF Migration</i>	Describes how to import content from Domino and Notes NSF files into Enterprise Vault archives.
<i>PST Migration</i>	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
<i>Utilities</i>	Describes Enterprise Vault tools and utilities.
<i>Registry Values</i>	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
<i>Help for Administration Console</i>	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>.

Introducing Enterprise Vault auditing

This chapter includes the following topics:

- [About Enterprise Vault auditing](#)

About Enterprise Vault auditing

Enterprise Vault includes flexible auditing that you can enable for individual Enterprise Vault servers. The auditing data is written to a SQL Server database - you can have a single audit database for all Enterprise Vault servers in a site.

Enterprise Vault auditing records the following:

- The time an event occurred
- The account that initiated the activity
- The archive in which an item was archived
- The category of the event, such as View, Archive, or Delete

You can enable auditing for a number of different types of event, showing for example, details of the following:

- Actions taken using the Administration Console
- Searches
- Viewing an item
- Deletions

For most types of event you can specify detail levels of Summary or Details, or both:

- Summary gives information about the event, such as the date and time, account used, vault used.
- Details lists more information, such as extracts from the content of a message, for example Subject, Mailbox Owner, and Folder.

You can view the audit database entries using SQL queries, or use the Audit Viewer utility.

Enterprise Vault provides PowerShell cmdlets for managing Enterprise Vault SQL databases. See the *PowerShell cmdlets* guide for more information.

Note that there will be a slight reduction in performance when you enable auditing. Auditing is disabled by default.

Setting up auditing

This chapter includes the following topics:

- [Setting up auditing](#)
- [Creating the audit database](#)
- [Configuring audit categories](#)
- [Starting or stopping auditing](#)
- [Tuning auditing](#)
- [Moving the auditing database](#)

Setting up auditing

[Table 3-1](#) summarizes the tasks that are required to set up auditing, and provides links to the sections where you can find more information.

Table 3-1 Steps to set up auditing

Steps	Task	More information
Step 1	Create the audit database.	One audit database is created for all of the Enterprise Vault servers in the site. See “Creating the audit database” on page 13.
Step 2	Select the categories to audit.	You configure audit categories on each Enterprise Vault server in the site. See “Configuring audit categories” on page 14.

Table 3-1 Steps to set up auditing (*continued*)

Steps	Task	More information
Step 3	Start or stop auditing.	You need to start or stop auditing on each Enterprise Vault server in the site. See “Starting or stopping auditing” on page 17.
Step 4	If necessary, tune auditing.	You can tune auditing by changing the number of connections that Enterprise Vault services can make to the audit database. See “Tuning auditing” on page 18.

There are registry settings associated with the configuration of Enterprise Vault auditing. If you change these registry settings directly using Regedit, instead of using the Enterprise Vault Administration Console, Enterprise Vault auditing cannot capture information about the user who makes the changes. If you want to record this information, configure Windows Registry Auditing for the settings under

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise
Vault\Admin\Auditing.

Note: Always configure Enterprise Vault auditing using the Enterprise Vault Administration Console. Do not change the associated registry values directly.

Creating the audit database

This section describes how to use the Administration Console to create the audit database.

It is important to apply appropriate security to the audit database. You should consider limiting the access to the database for very privileged users, such as the Vault Service account. For example, you may want to prevent the Vault Service account from removing or modifying Archive Permissions records in the audit database.

The Enterprise Vault databases contain roles that you can use to increase the database security in your environment. For information on how to use database roles to improve security on the audit database, see [Using sing SQL Database Roles in Enterprise Vault, Compliance Accelerator, and Discovery Accelerator](#).

Note: The audit database can grow to a large size, and it may sometimes be necessary to perform a rollover to a new database or remove entries from the database to reclaim some disk space. For more information, see the Enterprise Vault [SQL Best Practices](#) guide.

To create the audit database

- 1 In the left pane of the Administration Console, right-click the Enterprise Vault Directory and then, on the context menu, click **Enable Auditing**.
- 2 Under **Audit Database location**, click **Browse** to display the available locations for the audit database.
- 3 If you want to create a new folder for the audit database, click **New Folder**.
- 4 Click the location to use for the audit database, and then click **OK**.
- 5 Under **Transaction log location**, click **Browse** to display the available locations for the audit database transaction log.
- 6 If you want to create a new folder for the transaction log, click **New Folder**.
- 7 Click the location to use for the log, and then click **OK**.
- 8 Click **OK** to close the Configure Auditing dialog box.
- 9 Wait a few moments for Enterprise Vault to create the database.
- 10 When Enterprise Vault displays a message confirming that it has created the audit database, click **OK** to dismiss the message.

The audit database is created on the same SQL Server as the Enterprise Vault Directory database. However, you can move the audit database to another server, if required.

See [“Moving the auditing database”](#) on page 18.

Configuring audit categories

Audit categories identify the different types of information that auditing can collect. After you have created the audit database, you can use the Enterprise Vault Administration Console to select audit categories. All categories can record summary audit data, and some can also record detailed data.

Audit categories apply to the Enterprise Vault server that you select in the **Enterprise Vault Servers** container in the Administration Console. If there are multiple Enterprise Vault servers, you need to select each server in turn, and configure the audit categories for each server. It is good practice to set the audit categories consistently on all of the Enterprise Vault servers in the sites that are associated with the Enterprise Vault directory. Failure to do this will result in inconsistent audit

data in your environment. If you select the **Archive Permissions** category, it is particularly important to select this category on all of the Enterprise Vault servers.

When an Enterprise Vault administrator changes the auditing configuration, event ID 4288 reports whether auditing is running (enabled) or stopped (disabled), the status of each audit category, and the identity of the administrator who made the change. An audit database entry is also created with the same information.

You can modify the audit categories when auditing is running or stopped.

Table 3-2 Audit categories

Category	Description
Admin Activity	Configuration changes made in the Enterprise Vault Administration Console or Management Shell, such as adding a new task, creating archives, or enabling mailboxes.
Advanced Search	Searches performed, including the terms used and the number of items found.
Archive	Items being archived, either manually or on a scheduled run.
Archive Folder Updates	Archived items being moved to a different mailbox folder.
Archive Permissions	<p>Manual changes to user or group access permissions on an archive. Manual permissions are set on an archive in the Enterprise Vault Administration Console using the Archive Properties dialog box, or using the Enterprise Vault Policy Manager (EVPM) utility. If you select this category, you should select it on all of the Enterprise Vault servers in the site.</p> <p>Note that this auditing category does not capture changes to automatic access permissions on an archive. Automatic archive permissions are permissions that are set on the original content source, and synchronized to the Enterprise Vault archive. To capture this information, you must enable and configure auditing in the content source application. For example, access permission changes that a user makes on an Exchange Server mailbox are automatically synchronized to the associated Enterprise Vault archive. To capture these permission changes, you must enable and configure Exchange Server auditing on the Exchange Server that hosts the mailbox.</p>
Classification	Classification of archived items.
Delete	Archived items being deleted because their retention periods have expired, users have chosen to delete them, or third-party applications have requested their deletion for compliance with data protection legislation.

Table 3-2 Audit categories (*continued*)

Category	Description
Domino Archive	Any Domino archiving activity.
Domino Restore	Any Domino restore activity.
Exchange Synchronization	Records details of creation, modification, and deletion of Exchange managed content settings. Enterprise Vault records relevant details when it is configured to archive from Exchange managed folders and to synchronize with their managed content settings.
FS Archive	File System Archiving activity.
GetOnlineXML	Document retrieval into SharePoint Portal Server.
Indexing operations	When indexing subtasks for managing index volumes start and stop. Also records any critical errors that the subtasks encounter when processing indexes. The Manage Indexes wizard enables you to manage index volumes.
Move Archive	Details of individual Move Archive operations.
NSF Migration	Items being migrated from NSF files.
PST Migration	Items being migrated from PST files.
Restore	Archived items being restored.
Retention Category Updates	Changes to the retention category of archived items.
SPS Archive	SharePoint archiving activity.
Saveset Status	(For Support use.) Rarely used. Records whether a saveset file is available.
Subtask Control	The creation and modification of subtasks, such as the subtasks that control Move Archive operations.
Undelete	Deleted items that are recovered using the option Recover items on the Deleted Items tab of Archive Properties. Shortcuts recovered using the FSAUndelete utility are also recorded.
User	Your own auditing entries.
View	Viewing archived items, either as HTML or in their original formats.
View Attachments	Viewing of archived items from within SharePoint Portal Server.

To configure audit categories

- 1 In the Administration Console, expand the tree in the left pane until the Enterprise Vault Servers container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Right-click the computer for which you want to configure auditing, and click **Properties** on the context menu.
- 4 Click the **Auditing** tab.
- 5 Select or clear the audit categories.
[Table 3-2](#)
- 6 Click **OK** to save the changes you have made.

Starting or stopping auditing

To start or stop auditing you need to perform the following procedure on each Enterprise Vault server.

When auditing is started or stopped, event ID 42388 reports whether auditing is running (enabled) or stopped (disabled), the status of each audit category, and the identity of the administrator who made the change. When the Enterprise Vault Admin service starts, event ID 4286 is reported if auditing is running and event ID 4287 is reported if auditing is stopped. An audit database entry is also created with the same information.

To start or stop auditing

- 1 In the Administration Console, expand the tree in the left pane until the Enterprise Vault Servers container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Right-click the computer on which you want to start or stop auditing, and click **Properties** on the context menu.
- 4 Click the **Auditing** tab.
- 5 To start auditing on the Enterprise Vault server, select **Audit entries based on the following categories**.
To stop auditing on the server, clear this setting.
- 6 Click **OK** to save the changes you have made.

Tuning auditing

Each computer on which you enable auditing has a limited number of connections that it can make to the audit database. These connections are reused as needed. Auditing uses a pool of connections to the audit database. You can make Enterprise Vault audit record the level of usage of these connections and then, if necessary, you can modify the number of connections as required.

To tune auditing

- 1 In the Administration Console, expand the tree in the left pane until the **Enterprise Vault Servers** container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Right-click the computer for which you want to enable or disable connection information logging, and click **Properties** on the context menu.
- 4 Click the **Auditing** tab.
- 5 Click **Advanced**.
- 6 Select or clear **Log database information** to turn logging on or off.
- 7 If necessary, modify the number of connections for each Enterprise Vault service.
- 8 Click **OK**.
- 9 Restart the Enterprise Vault Admin service on the computer.

Moving the auditing database

You can move the auditing database to a different SQL Server if required, for example during disaster recovery. When you have moved the database, complete the following procedure on each Enterprise Vault server on which auditing is enabled.

To move the auditing database

- 1 Move the auditing database to the new SQL Server.
- 2 On the Enterprise Vault server, use the ODBC Data Source Administrator to select the new SQL Server on the EVAudit ODBC data source.
- 3 Test the data source when the ODBC Data Source Administrator gives you the opportunity.

Viewing the audit database entries

This chapter includes the following topics:

- [About viewing the audit database entries](#)
- [Viewing the audit database entries using Audit Viewer](#)
- [Viewing the audit database entries using SQL queries](#)

About viewing the audit database entries

You can view and filter the audit database entries using SQL queries. You can also use scripting to customize how the entries are processed and displayed.

Alternatively, Enterprise Vault provides the Audit Viewer utility, which lets you view and filter the audit entries.

Viewing the audit database entries using Audit Viewer

Audit Viewer lets you view and filter the data that is recorded in an Enterprise Vault audit database. You can specify the data that you want to view, sort the data, and copy it to the Windows Clipboard.

Using Audit Viewer to run a report on audit data

Follow the instructions in this section to open Audit Viewer and generate a report on the data in the auditing database.

Note: You must run this utility with Administrator privileges if the computer has User Account Control (UAC) enabled.

To use Audit Viewer to run a report on audit data

- 1
- In Windows Explorer, browse to the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`).
- 2
- Double-click `AuditViewer.exe`.
- 3
- In the Audit Viewer window, type or select the search criteria for the records that you want to view.

The following table provides information on each search term.

User Name	Specify the required user in the form <i>domain\username</i> .
Archive	Specify the name of the required archive. You can use the Enterprise Vault Administration Console to determine the name.
Category	Select a category of audit entries to search from the list. Audit Viewer lists only those categories that exist in the captured data.
Subcategory	<div>After you have selected a category, select a subcategory from the list.</div> <div><ul style="list-style-type: none">■ Item returns the summary information for a category.■ If you select Detailed as a category, the additional information is held in Information records.■ All returns both the summary and detailed records for selected categories.</div>
Date (From), Date (To)	Define a date range and time range to search the audit records.
Information contains	Type a keyword for which to search in the audit records.
Status	Select a status from the list for the records that you want to view.
Server	Select the Enterprise Vault server that is the target of this search.
Audit ID	Type a range of numbers to indicate the audit records that you want to view.
Order By	Select the attribute by which to order the results and whether you want Audit Viewer to list the results in ascending order or descending order.

Maximum Results Select whether to view all the results that the search finds or a portion of those results.

- 4 Click **Search** to generate the report.

Copying the search results from Audit Viewer

Audit Viewer displays the records that match your search criteria in the Search Results window.

Click a column heading to sort the records according to the entries in that column.

You can copy the contents of this window to another application, such as a spreadsheet application.

To copy the search results from Audit Viewer

- 1 In the Search Results window, highlight the records that you want to copy.
- 2 Right-click the records, and then click **Copy**.

You can also press Ctrl+A and Ctrl+C to copy all the search results to the Clipboard.

- 3 Paste the records into the destination document.

Changing Audit Viewer settings

You can change the auditing database that you want to search. Audit Viewer also provides the option to hide or show selected fields in the Search Results window.

To change Audit Viewer settings

- 1 In the main Audit Viewer window, click **Settings**.
- 2 In the Settings window, change the auditing database that you want to search. You can also select or clear the return fields that you want to show or hide.

Viewing the audit database entries using SQL queries

We recommend that you query the database view, **EVAuditView**, in the audit database. The SQL queries can filter audit entries based on criteria, such as a date range, user name, or ObjectID. See the Appendix to this document for a description of the format of audit database entries, and an explanation of the values in the EVAuditView columns for different types of audit entry.

See [“The format of audit database entries”](#) on page 31.

The procedure below shows you how to use SQL Server Management Studio to enter and run SQL queries. Later sections include example SQL queries that search database entries for item delete operations. You may need to run such queries to obtain evidence of item deletion, for example, to show compliance with data protection regulations.

See [“Auditing general delete operations”](#) on page 25.

Changes to archive access permissions are shown as Security Descriptor Definition Language (SDDL) strings. A script is shipped with Enterprise Vault to convert these strings to an array of permissions in a more user-friendly format.

See [“Retrieving audited changes to archive permissions in a user-friendly format”](#) on page 23.

To view the audit database entries using SQL Server Management Studio

- 1 Start the SQL Server Management Studio.
- 2 On the Standard toolbar, click **New Query**.
- 3 On the SQL Editor toolbar, select **EnterpriseVaultAudit** from the list of available databases.
- 4 Type a SQL query to retrieve the audit entries that you want.

This simple example query retrieves the audit entries from the database view, **EVAuditView**, in date order:

```
SELECT * FROM EVAuditView ORDER BY AuditDate DESC
```

Here is another example query. This example query filters entries based on a date range and user names.

```
USE EnterpriseVaultAudit

DECLARE @StartDateTime datetime
DECLARE @EndDateTime datetime

SET @StartDateTime = '2017-10-05 08:00:00'
SET @EndDateTime = '2017-10-06 08:00:00'

SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]
WHERE AuditDate BETWEEN @StartDateTime and @EndDateTime
AND UserName in ('Org\HSmith', 'Org\JDoe')
ORDER BY AuditID
```

- 5 Click **Execute** on the SQL Editor toolbar, or press F5 to run the command.

Retrieving audited changes to archive permissions in a user-friendly format

An administrator can change the manual permissions on an archive using the Permissions tab on the Archive properties, or using the Enterprise Vault Policy Manager (EVPN) utility. In audit database entries, changes to manual archive access permissions are shown as Security Descriptor Definition Language (SDDL) strings for Windows permissions, and XML for Domino permissions. An example PowerShell script, `ExampleEvPermissionsAuditHelper.ps1`, is included in Enterprise Vault to show you how you can convert these strings to an array of permissions in a more user-friendly format. The following information is included in the script output:

- Identity details of the archive.
- Name of the Enterprise Vault administrator who changed the permissions.
- A list of the old and new permissions for each administrator who has manual permissions set on the archive.

The example script is located in the folder, *Enterprise Vault_installation\Auditing*. You can run the script on your audit database, or modify it to use as part of your audit database processing. The Enterprise Vault Management Shell is not required to run this script.

The comments in the example script explain what the script does, the permissions needed to run the script, and the limitations of this example. You need to change values in the script for your environment.

The permissions available in the Archive properties dialog box and in EVPN are Read, Write, and Delete. These permissions equate to more granular permissions in audit database entries. [Table 4-1](#) shows the mapping between the permissions that are available to administrators, and the underlying permissions that are displayed in the audit database entries that are output by the example script.

Table 4-1 Mapping of available permissions to permissions output by script

Permissions in Archive properties and EVPN	Permissions output by example script
Read	READ_FOLDER READ_ITEM
Write	ADD_FOLDER ADD_ITEM CONTROL_FOLDER

Table 4-1 Mapping of available permissions to permissions output by script
(continued)

Permissions in Archive properties and EVPM	Permissions output by example script
Delete	DELETE_FOLDER DELETE_ITEM

Auditing for data protection compliance

This chapter includes the following topics:

- [Auditing general delete operations](#)
- [Auditing privileged delete operations](#)

Auditing general delete operations

Some data protection regulations, such as the European Union General Data Protection Regulation (GDPR), include the "Right to be Forgotten". This regulation supports requests to delete personal information that no longer needs to be held in an organization's storage system. You can use Enterprise Vault auditing to provide evidence that the information has been deleted.

This section describes how you can set up Enterprise Vault to support requests to delete specific information in Enterprise Vault. Example searches show how you can retrieve the audit entries that provide evidence of the item delete operations. The examples in this section relate to general delete operations in Enterprise Vault.

A Privileged Delete feature is available in Discovery Accelerator. This feature allows administrators with special privileges to delete items to comply with data regulations. A similar feature is also available to third-party applications that use the Enterprise Vault API. Enterprise Vault audit entries for these operations identify that the delete operation was performed as part of data regulation compliance. For this reason, the SQL searches and results for privileged delete operations are slightly different from those for general delete operations.

See "[Auditing privileged delete operations](#)" on page 29.

[Table 5-1](#) gives an example of the steps that you can take to provide audit database entries as evidence that specific data has been deleted from archives.

To facilitate searching, this example includes the use of the Enterprise Vault Classification feature. You can configure the Enterprise Vault classification feature to tag different types of information when it is archived. For example, Enterprise Vault classification can apply the tag, **evtag.category:PII**, to personally identifiable information (PII).

Table 5-1 Steps to provide evidence of item deletion

Step	Action	More information
1	Check that the site setting, Enable recovery of user deleted items , is not selected.	If "Right to be Forgotten" requests are likely, it is important that this site setting is not enabled. This ensures that items cannot be restored after the "Right to be Forgotten" request has been carried out.
2	Check that auditing is enabled, and the required audit categories are selected.	Enable Enterprise Vault auditing. In the properties of the Enterprise Vault server, the auditing categories that need to be enabled for this example are Advanced Search and Delete . The summary level is sufficient for the Delete category.
3	Search for the items to delete.	In this example, we use Enterprise Vault Search to search an Exchange Mailbox archive for the data to delete. Before performing the search, ensure that the administrator who performs the search has adequate permission on the user's archive to delete items. The search entered is: <code>'evtag.category:PII'</code> The actual search performed by Enterprise Vault Search is: <code>' (NOT sens:2) AND (evtag.category:PII) '</code> This means that any items marked as 'Private' in Outlook are not returned in the search; Enterprise Vault Search does this filtering automatically.
4	Use Enterprise Vault Search to delete all returned results.	In the search policy, ensure that item deletion is enabled. In Enterprise Vault Search, right-click the item to delete, and select Delete .
5	Repeat the same search in Enterprise Vault Search.	It is important to repeat the same search to show that the correct items were deleted.

Table 5-1 Steps to provide evidence of item deletion (*continued*)

Step	Action	More information
6	Search for the delete operation entries in the audit database.	<p>Extract the relevant part of the audit trail using suitable SQL queries. The search queries can be based on, for example, audit date, archive ID, and so on.</p> <p>See “Example query search for general item delete audit entries” on page 27.</p> <p>See “Example query search for privileged delete audit entries” on page 29.</p>

Example query search for general item delete audit entries

The following simple query retrieves from the audit database all Search and Delete entries within a specified time period.

```
USE EnterpriseVaultAudit
SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]
WHERE CategoryName in ('Search', 'Delete')
AND AuditDate BETWEEN '2017-10-05 08:27:48' and '2017-10-05 08:32:37'
ORDER BY AuditID desc
```

The following SQL query extends this simple query to filter on archive also. The archive information is stored in the Enterprise Vault directory.

```
DECLARE @ArchiveId varchar(112)
DECLARE @StartDateTime datetime
DECLARE @EndDateTime datetime

SET @ArchiveId = '1B29F35DAA512AC47A64558FDF7A614571110000example.local'
SET @StartDateTime = '2017-10-05 08:27:48'
SET @EndDateTime = '2017-10-05 08:28:37'

CREATE TABLE #ArchiveFolders
(
    VaultEntryId varchar(112)
)

INSERT INTO #ArchiveFolders
SELECT VaultEntryId
FROM [EnterpriseVaultDirectory].[dbo].[ArchiveFolderView]
WHERE ArchiveVEID = @ArchiveId
```

```
SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]
auditView LEFT JOIN #ArchiveFolders archFolder
ON archFolder.VaultEntryId = auditView.Vault
WHERE AuditDate BETWEEN @StartDateTime and @EndDateTime
AND CategoryName in ('Search', 'Delete')
ORDER BY AuditID
```

```
DROP TABLE #ArchiveFolders
```

[Table 5-2](#) shows example data returned by the SQL query of the audit database. The column titles relate to the database view, EVAuditView, in the audit database. The values in the column, **Example values (Search)**, show an audit entry created by the initial search for the items to delete. The values in the column, **Example values (Delete)**, show an audit entry created when the user, jdoe, deleted an item.

Given the steps in [Table 5-1](#), there would also be an audit entry for the final search showing that the item no longer exists. This audit entry is not included in [Table 5-2](#).

See the Appendix to this document for a description of the format of audit database entries, and an explanation of the values in the EVAuditView columns for different types of audit entry.

Table 5-2 Example audit entry values returned by the SQL query

EVAuditView column title	Example values (Search)	Example values (Delete)
AuditID	3582	3584
Status	SUCCESS	SUCCESS
AuditDate	31/08/2017 10:03:37	31/08/2017 10:03:44
UserName	example\jdoe The user who performed the search operation.	example\jdoe The user who performed the delete operation.
CategoryName	Search	Delete
SubCategoryName	Searches	Item
ObjectID (Saveset and/or Folder ID)		#142\$1610D28B10DB21647B11EEF479019B70B1110000example.local
Vault (Archive or Folder ID)	16454F118169EDE48822DC10CE69307CA1110000example.local	1610D28B10DB21647B11EEF479019B70B1110000example.local

Table 5-2 Example audit entry values returned by the SQL query (*continued*)

EVAuditView column title	Example values (Search)	Example values (Delete)
Info	Query '(NOT sens:2) AND (evtag.category:PII)', matching '8' entries, viewing range '1' to '100'	
MachineName	EVServer1	EVServer1

Auditing privileged delete operations

By assigning the role of Regulatory Reviewer to selected Discovery Accelerator client users, you can now permit them to delete items permanently from Enterprise Vault archives. The Privileged Delete permission that is associated with the role enables these users to mark items in the case review set for deletion from the archives. For more information about the Privileged Delete feature, see the *Discovery Accelerator Administrator's Guide*.

A compliance delete feature is also available for third party applications that use the Enterprise Vault API. The user under which the third-party application runs must be assigned to the Enterprise Vault Compliance Delete Application role.

Enterprise Vault auditing records additional information about compliance deletions made using Privileged Delete in Discovery Accelerator and compliance delete in third-party applications that use the Enterprise Vault API.

You can run SQL queries on the audit database to retrieve information about compliance deletion operations.

Example query search for privileged delete audit entries

The following example query searches the audit database for item delete operations between the dates that you specify:

```
USE EnterpriseVaultAudit
GO
SELECT * FROM EVAuditView WHERE CategoryName = 'Delete' AND
SubCategoryName = 'Information' AND AuditDate BETWEEN
CONVERT(datetime, 'mm-dd-yyyy', 110) and
CONVERT(datetime, 'mm-dd-yyyy', 110)
```

[Table 5-3](#) shows example values of an audit entry returned by this query.

Table 5-3 Example audit entry values returned by the SQL query

EVAuditView column title	Example values (Delete)
AuditID	4
Status	SUCCESS
AuditDate	2018-02-02 17:01:56.583
UserName	example\vs The user who performed the delete operation. For items that are were deleted by the Discovery Accelerator Privileged Delete feature, the UserName column displays the name of the Vault Service account. For items that were deleted by a third-party application, this is the user that is assigned to the Compliance Delete Application role.
CategoryName	Delete
SubCategoryName	Information
ObjectID	201802017502363~201802011626030000~Z~A158658C6FBE60B76 The saveset ID of the item that was deleted.
Vault	600B5AA958C24411F9D0B892B91F5E4393B33DB7F88B8E551110000VS1 The archive that contained the item.
Info	<Delete ObjectType="Item" ObjectName="(null)" "> <Property Name="EV_API_DELETION_LEVEL"> <Current Value="DELETION_LEVEL_COMPLIANCE"/> </Property> </Delete> The deletion level DELETION_LEVEL_COMPLIANCE denotes that the item was deleted using Privileged Delete in Discovery Accelerator or compliance delete in a third-party application that uses the Enterprise Vault API.
MachineName	EVServer1

Format of audit database entries

This appendix includes the following topics:

- [The format of audit database entries](#)

The format of audit database entries

In Enterprise Vault 12.3, auditing of administrative activity (**Admin Activity** auditing category) has been enhanced. In particular, the quality of information relating to administrative activity in the following areas is significantly improved:

- Exchange, SMTP, and Search policies
- Exchange and SMTP tasks
- Exchange and SMTP targets
- Exchange Message Classes
- Archives

Improvements have also been made to the auditing of roles-based administration, vault store and partition administration, and advanced settings.

The improved information is available for activities performed using the Administration Console, or PowerShell cmdlets.

Note: Veritas is enhancing Enterprise Vault auditing over several releases. The detailed information in this Appendix may change in future releases.

The EVAuditView database view in the Auditing database can be used to display audit entries and consists of the following columns:

Table A-1 Description of EVAuditView columns

Column title	Description of content
AuditID	A unique identifier for the audit entry.
Status	SUCCESS or FAILURE. Whether the operation has completed successfully or failed.
AuditDate	Date and time of the action or operation that caused the audit entry.
UserName	The user who performed the action.
CategoryName	The audit category, as defined in the Computer Properties of the Enterprise Vault server.
SubCategoryName	A more specific categorization of the audit entry.
ObjectID	The ID of the entity that was changed, for example, Saveset ID, Site ID, Archive ID.
Vault	For high volume audits only, this often contains the Archive ID or ArchivePoint ID.
Info	Freeform text providing more information on the action performed. In Enterprise Vault 12.3 and later, much more detail about the audited action is provided in this column. The content of this column in different audit entries is the main topic of this Appendix.
MachineName	The machine from which the audit entry was generated.

A new format has been introduced for the `Info` column, that allows information about the audited action to be displayed in a structured and consistent way. The remainder of this Appendix explains the content of the `Info` column in a variety of audit entries. Note that the full audit entry also contains the information listed above, such as the date and time, the user who performed the action, and the ID of the entity that was changed.

We recommend that you use SQL queries to view and filter audit entries based on criteria such as a date range, user name, or ObjectID.

To return formatted XML in the results, use a query like the following:

```
USE EnterpriseVaultAudit
SELECT TOP 50 ObjectID, AuditDate, UserName,
    TRY_CAST(info AS XML) AS infoXML
FROM EVAuditView
ORDER BY auditid DESC
```


Info content in simple audit entries

The following example shows the content of the `Info` column in an audit entry that was created when a setting in an Exchange Mailbox policy was changed. [Table A-2](#) explains the values included.

```
<Update ObjectType="ExchangePolicyView"
  ObjectName="Exchange Mailbox Policy 2">
  <Property Name="ProcessUnreadMail">
    <Previous Value="0" />
    <Current Value="1" />
  </Property>
  <Property Name="ProcessUnreadMail:TextValue">
    <Previous Value="Off" />
    <Current Value="On" />
  </Property>
</Update>
```

Table A-2 Description of XML fields in the example

XML field	Description
Update	The type of action. This is usually Create, Update, or Delete.
ObjectType	The type of entity that the action affected. This is often the name of the database table or view that changed. However, in some entries a friendlier name is provided.
ObjectName	The name of the entity that changed. <code>ObjectName</code> may not be populated if there is no appropriate value.
Property Name	<p>The name of a property relating to the entity. (See note 1.)</p> <p>For Create and Delete operations, most properties are listed because they have all gained or lost a value. (See note 2.)</p> <p>For Update operations, only changed properties are included. (See note 3.)</p> <p>:TextValue at the end of the Property Name field indicates that the following values are textual values for the setting. In the example, the textual values shown for the values "0" and "1" are "Off" and "On".</p>
Previous Value	The value of the property before the action was taken.
Current Value	The value of the property after the action was taken.

Notes

- 1 The name is often the one used in the database, so it may not match exactly the name in the user interface.
- 2 To avoid unnecessary bloating of the audit trail, some properties that change very frequently are not included, for example, the size of an Exchange mailbox.
- 3 Extra properties are occasionally included for context. This also applies to other types of audit entry.

Info content for composite properties

For some settings in the Enterprise Vault database, multiple settings are represented by a single value. The audit entry splits these out into separate properties. In `Update` entries, typically only the settings that have changed are displayed.

The following example `Info` content was generated in an audit entry after changing the settings, **Include banner** and **Include link to archived item**, on the **Shortcut Content** tab of the Exchange Mailbox policy. These two settings are stored as a single value in the Enterprise Vault database.

```
<Update ObjectType="ExchangePolicyView"
  ObjectName="Exchange Mailbox Policy 2">
  <Property Name="excShortcutDetail">
    <Previous Value="1000005" />
    <Current Value="1000029" />
  </Property>
  <Property Name="excShortcutDetail:IncludeArchivedBanner">
    <Previous Value="False" />
    <Current Value="True" />
  </Property>
  <Property Name="excShortcutDetail:IncludeLinkToArchivedItem">
    <Previous Value="False" />
    <Current Value="True" />
  </Property>
</Update>
```

As you can see, information about the **Include banner** and **Include link to archived item** settings are displayed as separate properties.

Info content when multiple settings are stored in a single property

The following example `Info` content was generated in an audit entry when an SMTP target was deleted.

```

<Delete ObjectType="SmtptargetViewEx"
  ObjectName="JDoe@example.com">
  <Property Name="TargetId">
    <Current Value="19" />
  </Property>
  <Property Name="Address">
    <Current Value="JDoe@example.com" />
  </Property>
  <Property Name="poName">
    <Current Value="Default SMTP Policy" />
  </Property>
  <Property Name="RetentionCategoryName">
    <Current Value="RetCat01" />
  </Property>
  <Property Name="poPolicyEntryId">
    <Current Value="1781F4D98B1045F438445AC9
      8AD9579331s10000ev.local" />
  </Property>
  <Property Name="RetentionCategoryId">
    <Current Value="141E6B5A255237C4D83BB499
      390F27F091b10000ev.local" />
  </Property>
  <Property Name="ArchivingEnabled">
    <Current Value="1" />
  </Property>
  <Property Name="TargetType">
    <Current Value="1" />
  </Property>
  <Property Name="ArchiveInformation">
    <Current Value="<AI tn="JDoe@example.com" tid="19"
      an="Archive1" at="2049" aid="1868FD2720BFF62
      4483309845BDCCFEDB1110000ev.local" vs="Store1"
      ev="ev.local"/><AI tn="JDoe@example.com" tid=
      "19" an="Archive2" at="2049" aid="151D27
      0BA9638354DBE2B02FBFF7AF25C1110000ev.local" vs="Store1"
      ev="ev.local"/><AI tn="JDoe@example.com" tid="19"
      an="Archive3" at="2049" aid="13C3DC68A1FB836
      479CA542E4AE0CF9761110000ev.local" vs="Store2"
      ev="ev.local"/>" />
  </Property>
</Delete>

```

The `ArchiveInformation` property contains XML that gives details of three archives that were assigned to the SMTP target.

To make the information in the `ArchiveInformation` property more readable, a separate audit entry is created for each archive. The example below shows the audit entry for `Archive3` in the `ArchiveInformation` property above.

```
<Delete Object Type="SmtptargetViewEx:ArchiveInformation"
ObjectName="JDoe@example.com">
  <Property Name="TargetAddress">
    <Current Value="JDoe@example.com" />
  </Property>
  <Property Name="TargetId">
    <Current Value="19" />
  </Property>
  <Property Name="ArchiveName">
    <Current Value="Archive3" />
  </Property>
  <Property Name="ArchiveType">
    <Current Value="2049" />
  </Property>
  <Property Name="ArchiveId">
    <Current Value="13C3DC68A1FB836479CA542
      E4AE0CF9761110000ev.local" />
  </Property>
  <Property Name="VaultStoreName">
    <Current Value="Store2" />
  </Property>
  <Property Name="EvServer">
    <Current Value="ev.local" />
  </Property>
</Delete>
```

Splitting an audit entry into multiple entries is used where it provides additional clarity. Other examples where multiple audit entries may be created include roles-based administration updates, and the administration of X-Headers in SMTP policies.