



Enterprise Vault Whitepaper

Monitoring and Reporting

This document provides an overview of the different ways that Enterprise Vault logs events and the different tools available to monitor Enterprise Vault.

If you have any feedback or questions about this document please email them to IIG-TFE@symantec.com stating the document title.

This document applies to the following version(s) of Enterprise Vault:
2007, 8.0, 9.0, and 10.0

Document Control

Contributors

Who	Contribution
Evan Barrett	Author
Andy Joyce and Mark Olsen	Reviewers

Revision History

Version	Date	Changes
1.0	April 2010	Initial Release
2.0	November 2010	Updates for EV 9.0
3.0	January 2013	Updates for EV 10.0.3

Related Documents

Document Title	Version / Date
Advanced Strategies for Monitoring Enterprise Vault http://www.symantec.com/docs/HOWTO74545	March 2012

Table of Contents

Document Overview	1
Enterprise Vault Logs and Monitoring Databases	2
The Windows Event Viewer	2
The Monitoring Database	3
The Auditing Database	4
Enterprise Vault Services	5
Services Overview	5
The Enterprise Vault Admin Service	5
The Enterprise vault Directory Service	7
The Enterprise Vault Storage Service	7
The Enterprise Vault Indexing Service	8
The Enterprise Vault Shopping Service	8
The Enterprise Vault Task Controller Service	8
Enterprise Vault Operations Manager	9
Overview	9
Installing and Configuring	9
The Operations Manager Web Page	9
Enterprise Vault Monitoring	9
Exchange Server Monitoring	11
Domino Server Monitoring	13
Configuration	13
Enterprise Vault Reporting	15
Overview	15
Installing and Configuring	16
Accessing Enterprise Vault Reporting	17
System Status	19
Overview	19
Installing and Configuring	21
Interacting with System Status	21
Enterprise Vault Online	23
Monitoring Using Microsoft Operations Manager	24
Overview	24
Installing and Configuring	24
Optional Configuration	25
Monitoring Using System Center Operations Manager 2007 and 2012	26
Overview	26
Enterprise Vault 10.0.2 and Earlier	26
Enterprise Vault 10.0.3 and Later	26
Installing and Configuring – Enterprise Vault 10.0.2 and Earlier	27
Optional Configuration (Enterprise Vault 10.0.2 and Earlier)	27
In Conclusion	28

Document Overview

Monitoring an Enterprise Vault environment is essential for the efficient operation of an Enterprise Vault environment. As an Enterprise Vault administrator or operator, what are the Enterprise Vault services and tasks should be monitored? How can I monitor these services and check for any issues? How can I report on various aspects of Enterprise Vault?

The first few sections of this whitepaper will review the way that Enterprise Vault logs events as well as describe the various Enterprise Vault services and their functions within an Enterprise Vault environment. There are also recommendations on how to monitor and what frequency to review these processes.

The remainder of the document will cover the different tools for monitoring and reporting available from Symantec for Enterprise Vault. Although it is not necessary to install or use all of these tools, it will make the monitoring and reporting on Enterprise Vault an easier task. The tools that will be discussed in this whitepaper include Enterprise Vault Operations Manager, Enterprise Vault Reporting (using SQL Reporting Services), System Status, Enterprise Vault Online, using MOM/SCOM, and Symantec OpsCenter.

Enterprise Vault Operations Manager (EVOM) is a web-based utility for monitoring Enterprise Vault Environments. EVOM allows the Enterprise Vault administrator or operator to quickly glance at the overall status of Enterprise Vault services and tasks.

Enterprise Vault Reporting is an optional reporting tool that provides detailed reports on various aspects of an Enterprise Vault environment. EV Reporting uses Microsoft SQL Server Reporting Services.

System Status, a new feature offered with Enterprise Vault 8.0SP4, provides enhanced monitoring and alerting for Enterprise Vault. The Enterprise Vault administrator or operator will easily be able to see alerts using the Enterprise Vault Administration Console (VAC).

Enterprise Vault Online, a new feature offered with Enterprise Vault 8.0SP4, offers the Enterprise Vault administrator or operator an easy way to access frequently accessed and visited web sites. Accessible via the Enterprise Vault Administration Console, Enterprise Vault Online is its own container providing links to items such as Symantec Support and the Enterprise Vault compatibility guide.

Microsoft Operations Manager and System Center Operations Manager are products from Microsoft that monitor datacenter environments. Enterprise Vault has the ability to integrate with these tools.

This document is not intended to describe every potential issue that may arise in Enterprise Vault nor provide a troubleshooting guide, but rather educate the Enterprise Vault administrator on how

Enterprise Vault records events, how to proactively monitor Enterprise Vault, and how to report on Enterprise Vault environments.

Enterprise Vault Logs and Monitoring Databases

The Windows Event Viewer

Enterprise Vault will create two event logs on a Windows system, “Symantec Enterprise Vault” and “Symantec Enterprise Vault Converters”. The Symantec Enterprise Vault event log is the main log for Enterprise Vault and will contain the bulk of events. These event levels will range from informational, to warning, to error and should be one of the first locations to monitor in the event of an issue with an Enterprise Vault server. Warnings and errors listed in the event logs provide critical information on the state of the Enterprise Vault environment and should be monitored and reviewed at least several times per day (or more frequently) for optimal Enterprise Vault operation and health.

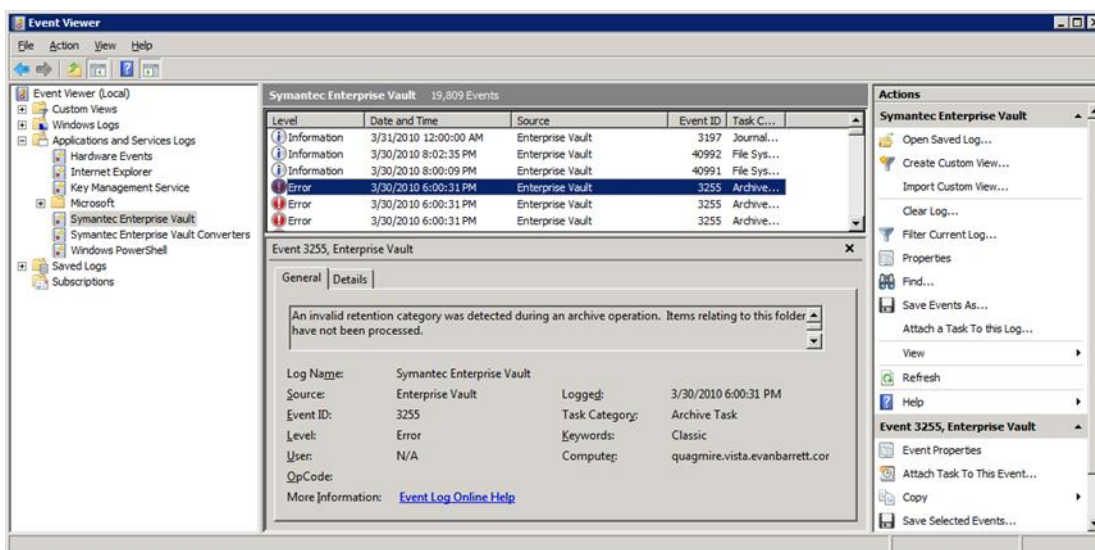


Figure 1 - The Enterprise Vault Event Log

The Symantec Enterprise Vault Converters event log (as shown in Figure 2) will display events associated with converting archived content. If Enterprise Vault is not able to convert an item (such as a Word or PDF document or some other type of object) to HTML and/or text, an event will be logged here.

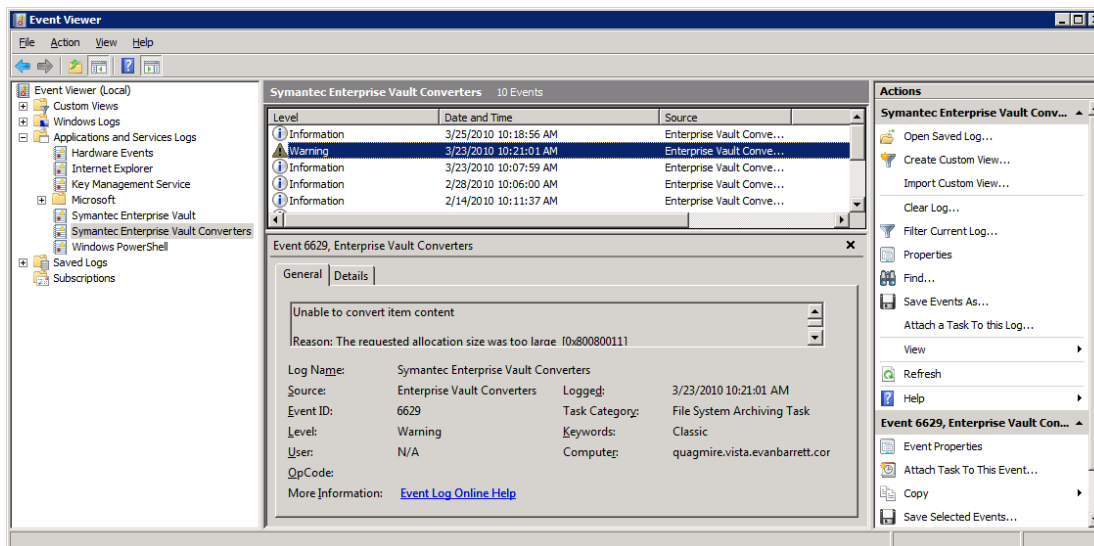


Figure 2 - The Enterprise Vault Converters Event Log

The Monitoring Database

The Enterprise Vault monitoring SQL database is created when the Enterprise Vault Configuration wizard is initiated on the first server in the Enterprise Vault directory structure. This database will contain a wide variety of data collected from Enterprise Vault servers. For data to be collected and stored in this database, an Enterprise Vault site must be enabled for monitoring. The data collected and stored in the monitoring database can be used by other tools which are explained in more detail later on in this document.

Monitoring can be enabled or disabled for a site using the Enterprise Vault Administration Console (VAC). In the VAC, bring up the properties for the site by right-clicking on the site name and selecting Properties. In the Properties window, click on the Monitoring tab. To enable monitoring, make sure that “Enable monitoring for this site” is checked (as illustrated in Figure 3). The administrator also has the ability to select which alerts should be enabled for monitoring.

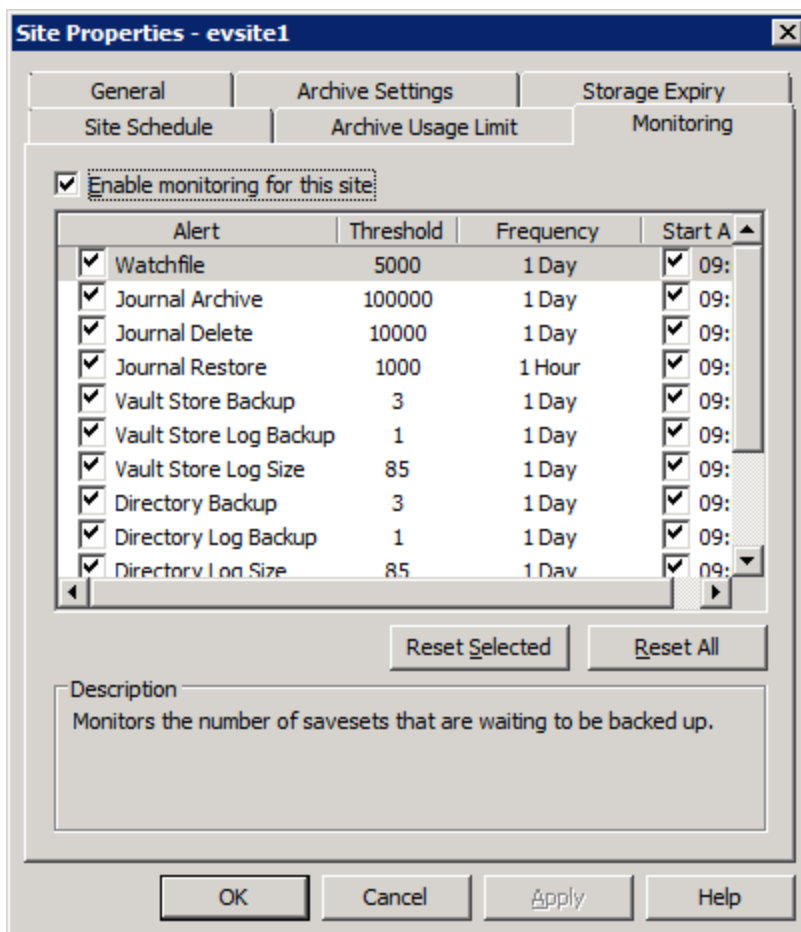


Figure 3 – Enabling Monitoring for an Enterprise Vault Site

The Auditing Database

The Auditing database contains a log of all events that occur in an Enterprise Vault directory environment such as archiving an item, an administrator making changes to an archiving policy, restoring an archived item, searches, or an item being deleted from an archive to name a few. An administrator or auditor can search for events in this database to determine when a particular event occurred.

Auditing is not enabled by default. To enable auditing, the Enterprise Vault administrator must use the Enterprise Vault Administration Console (VAC). In the VAC, right-click on the **Directory on <server_name>** and select Enable Auditing. In the Configuring Auditing wizard, specify the paths for the database and log files and click on OK. A pop-up window will appear once the database has been created. The Enterprise Vault administrator must be logged in as the Vault Service Account (VSA) in order to enable auditing.

To view or search for contents in the auditing database, Enterprise Vault comes with a program called AuditViewer.exe. This file is located in the Enterprise Vault installation directory (by default, C:\Program Files\Enterprise Vault or C:\Program Files (x86)\Enterprise Vault). It should be noted that items will only be recorded in the audit database from the point at which the auditing database was created. For example, if you created the auditing database today, you would not be able to search for items in the audit database for events that happened yesterday.

Enterprise Vault Services

Services Overview

There are up to six Enterprise Vault services that can run on an Enterprise Vault Server. These services include the Admin Service, Directory Service, Storage Service, Indexing Service, Shopping Service, and the Task Controller Service. A description of each service and its role in Enterprise Vault is described in this section. Figure 4 provides a high level overview the services and their dependencies.

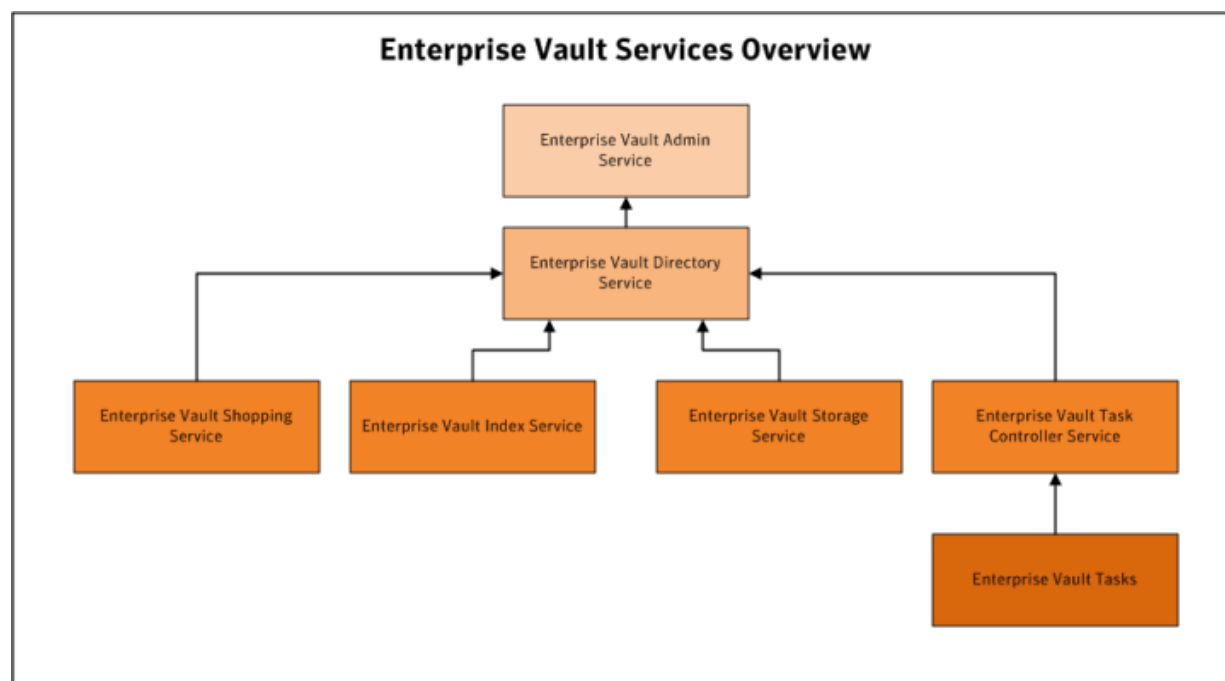


Figure 4 - Enterprise vault Services Overview

The Enterprise Vault Admin Service

All other Enterprise Vault services rely on the Admin Service to be started. One of the tasks of the Admin Service is to monitor various Enterprise Vault resources (such as free disk space, free virtual memory, and the number of items on system message queues) as well as Enterprise Vault services and tasks. It has the ability to write events to the event log and monitoring database (if enabled).

The Admin Service will monitor the Windows event log for events from other Enterprise Vault services. If there are more than X amount of errors in the event log in the last Y seconds of which Z% are from Enterprise Vault, the Admin Service will shutdown all Enterprise Vault services to prevent damage to Enterprise Vault. By default, X=500, Y=7200, and Z=90. To change these default settings, there are three registry settings to consider as detailed in Table 1.

Location	Setting Type	Description
HKLM\SOFTWARE\KVS\Enterprise Vault\AdminService\Warning	DWORD	The Admin Service checks the Enterprise Vault Event Log for errors every PollingInterval seconds (registry setting). If the number of entries since the previous check is larger than that specified in the Warning registry setting, the Admin Service calculates the percentage of errors that have come from Enterprise Vault. If this percentage is larger than that specified by the Critical registry setting, the Admin Service will shut down Enterprise Vault.
HKLM\SOFTWARE\KVS\Enterprise Vault\AdminService\PollingInterval	DWORD	The Admin Service checks the Enterprise Vault log periodically for errors. If too many errors have occurred since the last check, the Admin Service shuts down Enterprise Vault. PollingInterval specifies how often the Admin Service checks the Enterprise Vault Event Log for errors.
HKLM\SOFTWARE\KVS\Enterprise Vault\AdminService\Critical	DWORD	The Admin Service checks the Windows Application Log for errors every PollingInterval seconds (registry settings). If the proportion of error log entries is larger than the percentage specified by Critical, the Admin Service will shut down Enterprise Vault.

Table 1 - Enterprise Vault Admin Service Registry Settings for Monitoring

For more detailed information on other Admin Service registry settings, please review the Registry Settings guide applicable to the version of Enterprise Vault in the environment.

The monitoring of Admin Service events in the event log should be done often by the administrator or operator. Any warnings or errors should be reviewed and corrected as soon as possible. Failure to take corrective action may result in the failure of Enterprise Vault in general.

The Enterprise vault Directory Service

The Enterprise Vault Directory Service is a critical component of every Enterprise Vault server. It facilitates communications between Enterprise Vault services/tasks and various Enterprise Vault databases that reside on the Microsoft SQL Server. All other Enterprise Vault services (except for the Enterprise Vault Admin Service) depend on the Directory Service to be started. The Directory Service will record events to the event log such as the starting and stopping of the service as well as other events around communications with various databases on Microsoft SQL Server.

The monitoring of Directory Service events in the event log should be done hourly. Events logged that are of a warning or error nature from the Directory Service should immediately be reviewed and corrected as all other Enterprise Vault functionality may be affected by issues with the Directory Service.

The Enterprise Vault Storage Service

The Enterprise Vault Storage Service manages the vault stores and archives on the computer where it is running. If there are no vault stores configured on the Enterprise Vault server, the service is not critical. The functions of the service include the following:

- The Storage Service is responsible for converting content to be archived to HTML and/or text (if possible) which the Indexing Service uses to create the index for the archive.
- The service will also compress and store the original item and the text/HTML copy (if applicable) to the vault store partition.
- It processes restore requests from retrieval tasks.
- With Enterprise Vault 8.0 and later, the Storage Service will monitor vault store partitions and identify which partitions are eligible for partition rollover.
- The service responds to requests to view archived content and can provide an HTML preview of the item (if available)
- The service is also responsible for deleting archived content which can be initiated via a user, Enterprise Vault administrator, or through expiry
- The service facilitates storing and recalling of migrated content to tertiary devices such as NetBackup

The Storage Service will log events to event log when the service stops and starts as well as when other events dealing with storage are encountered. The administrator or operator should monitor Storage

Service events on an hourly basis. Events that are at a warning or error level should be dealt with immediately as they may indicate issues with storing and recalling archived content.

The Enterprise Vault Indexing Service

The Enterprise Vault Indexing Service is responsible for the management of the indexes for archived data. If the Enterprise Vault server will not participate in indexing, the service is not critical. The functions of the Indexing Service include the following:

- When initiated from the Storage Service, the Indexing Service will index items as they are being archived. Each archive will have its own index.
- If an index is out of date, the service will automatically update the index.
- The service facilitates search requests from Enterprise Vault web access components and returns results matching the search request (if any).

The Indexing Service will log events to the event log when the service stops and starts as well as when other events dealing with indexing arise. The administrator or operator should monitor for Index Service events at least once a day. Events that are at a warning or error level should be dealt with as soon as possible as they may indicate issues with indexing archived content and with searches.

The Enterprise Vault Shopping Service

The Enterprise Vault Shopping Service manages selected items to be restored when using Browser Search or Archive Explorer. The service will log events in the event log when the service starts and stops as well as when other issues arise. The administrator or operator should monitor Shopping Service events at least once per day. Events that are warnings or errors should be reviewed and corrected as soon as possible as these events may indicate issues with restoring selected data from browser search or Archive Explorer.

The Enterprise Vault Task Controller Service

The Enterprise Vault Task Controller Service controls all provisioning, archiving, and retrieval tasks for Enterprise Vault. Each task will record its own events in the event log and will be identified by having “Task” on the end when listed in the Task Category (such as “Archive Task” or “Exchange Provisioning Task”) of the event log. These task events should be monitored at least daily for warnings and errors and should be dealt with as soon as possible to correct any issues that may be affecting archiving and restoring of content.

Enterprise Vault Operations Manager

Overview

Enterprise Vault Operations Manager, or EVOM for short, is a web-based utility that provides monitoring of Enterprise Vault services and tasks, Exchange Server monitoring, Domino server monitoring, and the ability to configure thresholds for warning and critical alerts. This feature was first available with Enterprise Vault 6.0.

EVOM provides a quick of view of the current status of Enterprise Vault and should be reviewed as often as possible to identify any potential issues that may be present in an Enterprise Vault environment. Correcting these issues will ensure a more operational and healthy environment.

Installing and Configuring

EVOM is installed as a separate component. Only one instance of EVOM is required per Enterprise Vault site and must be installed on at least one Enterprise Vault server. For monitoring to properly work, the Enterprise Vault server will need to have the Enterprise Vault configuration wizard completed so that Enterprise Vault services have been configured.

EVOM will also require Internet Information Services (IIS) 6.0 or later and must not be locked down. If EVOM will be installed on Windows 2003 x64 Editions, IIS must be set to run in 32-bit mode. Please see <http://support.microsoft.com/?kbid=894435> for more information.

EVOM requires an Active Directory user account under which to run. It is recommended that this user be dedicated to EVOM. The account does not need to have an email account set up nor does the account require any Windows administrative privileges. When configuring this user, make sure to set the account so that the password never expires.

For more detailed information on installing Enterprise Vault Operations Manager, please review the Installing and Configuring Guide specific to the version of Enterprise Vault for your environment.

The Operations Manager Web Page

EVOM can be accessed by point a web browser to the Enterprise Vault server running EVOM. For example: `http://<EVServerAlias>/MonitoringWebApp`. Once the page has loaded, the summary page will appear.

Enterprise Vault Monitoring

The summary page will show an overview of each Enterprise Vault server in the selected site. The state of services and tasks (such as running or stopped) as well as performance counters are also shown.

EVOM will break out which archiving tasks are currently running on each Enterprise Vault server. An example of how the page may look is shown in Figure 5.

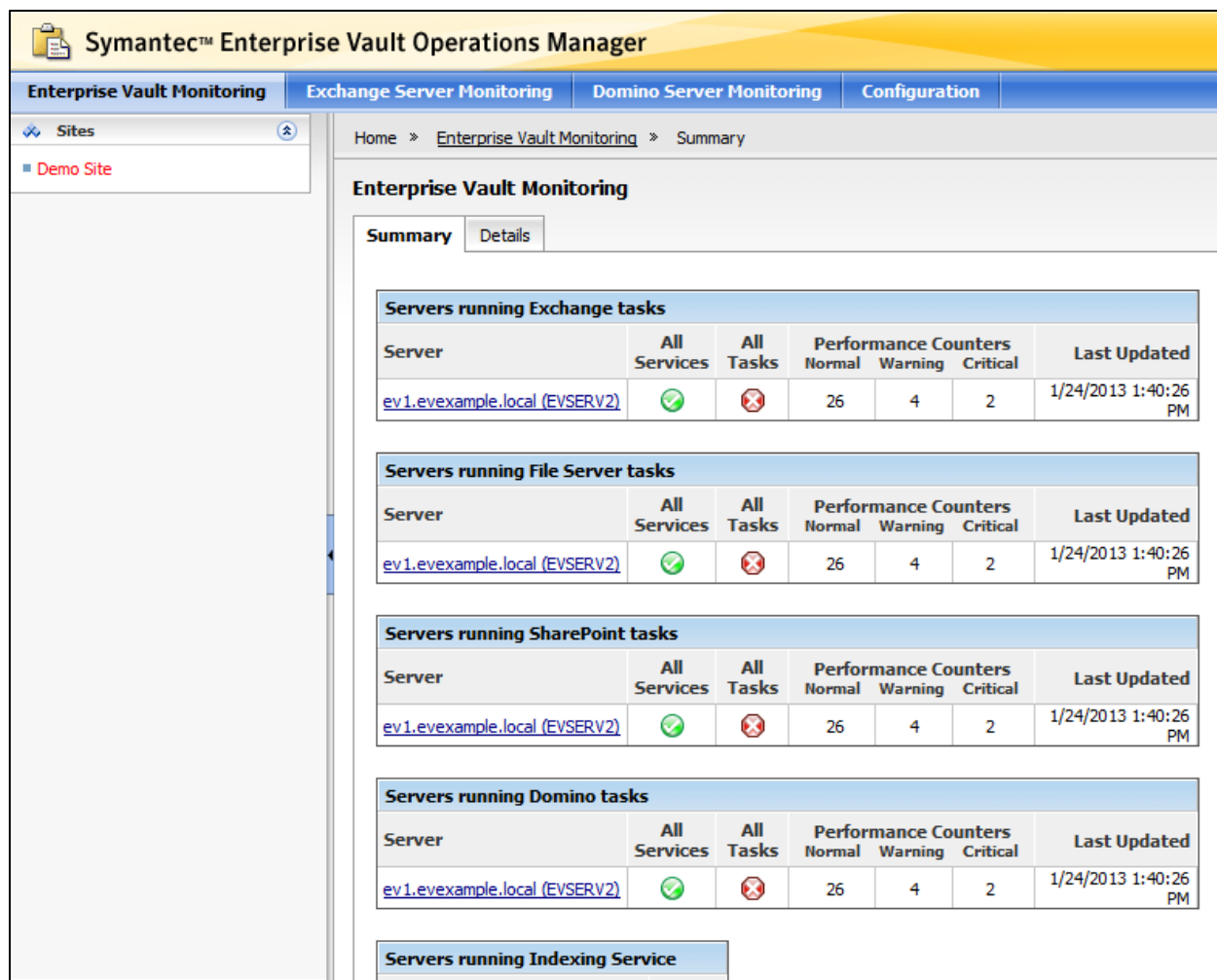


Figure 5 - EVOM Monitoring Web Page

Clicking on the **Details** sub tab will provide more details on Enterprise Vault services and tasks as well as detailed information on server properties such as disk space, memory, and CPU utilization for a selected Enterprise Vault server as shown in Figure 6.

Enterprise Vault Monitoring		
Summary	Details	
<div style="border: 1px solid black; padding: 2px;"> ev1.evexample.local (EVSERV2) (Last updated: 1/24/2013 2:08:45 PM) </div>		
Services		
Service	Status	Last Updated
Task Controller Service	Running	1/24/2013 1:55:22 PM
Indexing Service	Running	1/24/2013 1:55:22 PM
Storage Service	Running	1/24/2013 1:55:22 PM
Shopping Service	Running	1/24/2013 1:55:22 PM
Tasks		
Task	Status	Last Updated
Exchange Journaling Task for EVSERV3	Stopped	1/24/2013 1:55:22 PM
PST Collector Task	Stopped	1/24/2013 1:55:22 PM
Exchange Provisioning Task for evexample.local	Stopped	1/24/2013 1:55:22 PM
Index Administration Task	Stopped	1/24/2013 1:55:22 PM
SharePoint Task	Stopped	1/24/2013 1:55:22 PM
PST Locator Task	Stopped	1/24/2013 1:55:22 PM
Domino Mailbox Archiving Task	Stopped	1/24/2013 1:55:22 PM

Figure 6 - Details Sub Tab

Exchange Server Monitoring

The Exchange Server Monitoring tab provides details on each Microsoft Exchange server that has been configured for journal archiving. The summary sub tab provides a high-level overview for each configured Exchange server (Figure 7). The Details sub tab will provide more granular view of information for a selected Exchange server (Figure 8). EVOM will provide statistics on the amount of emails and their sizes over the past hour for each configured journal archive. If any of the monitored settings exceed the defined warning or critical thresholds, EVOM will change the status for the alert from Normal to either Warning or Critical.

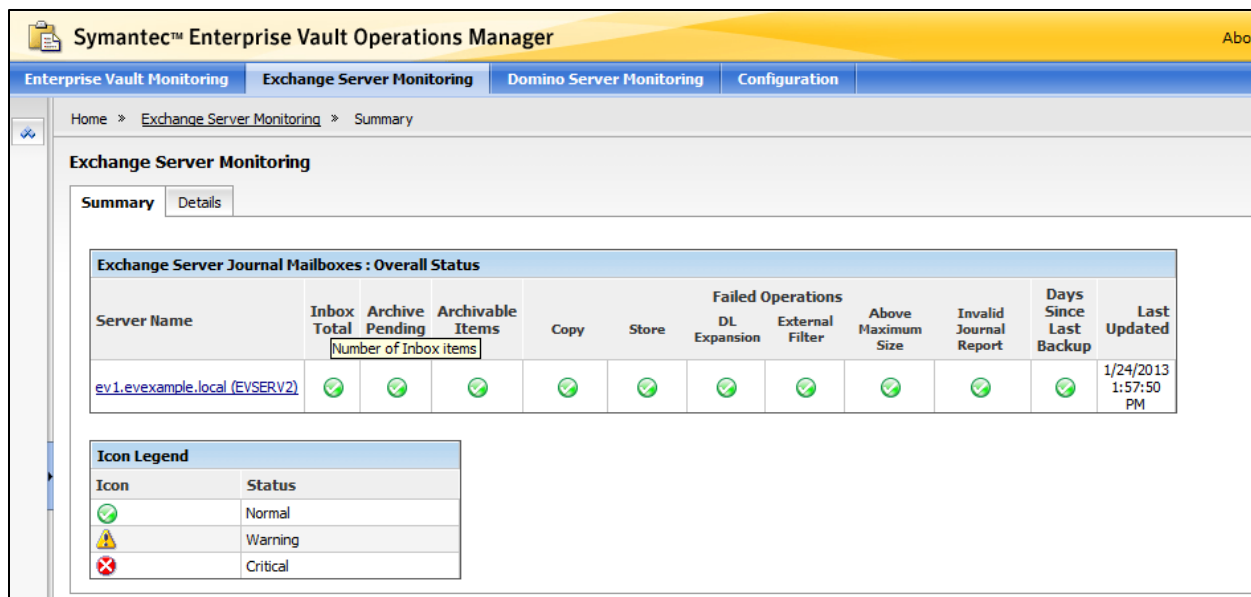


Figure 7 - Exchange Server Monitoring Summary Page

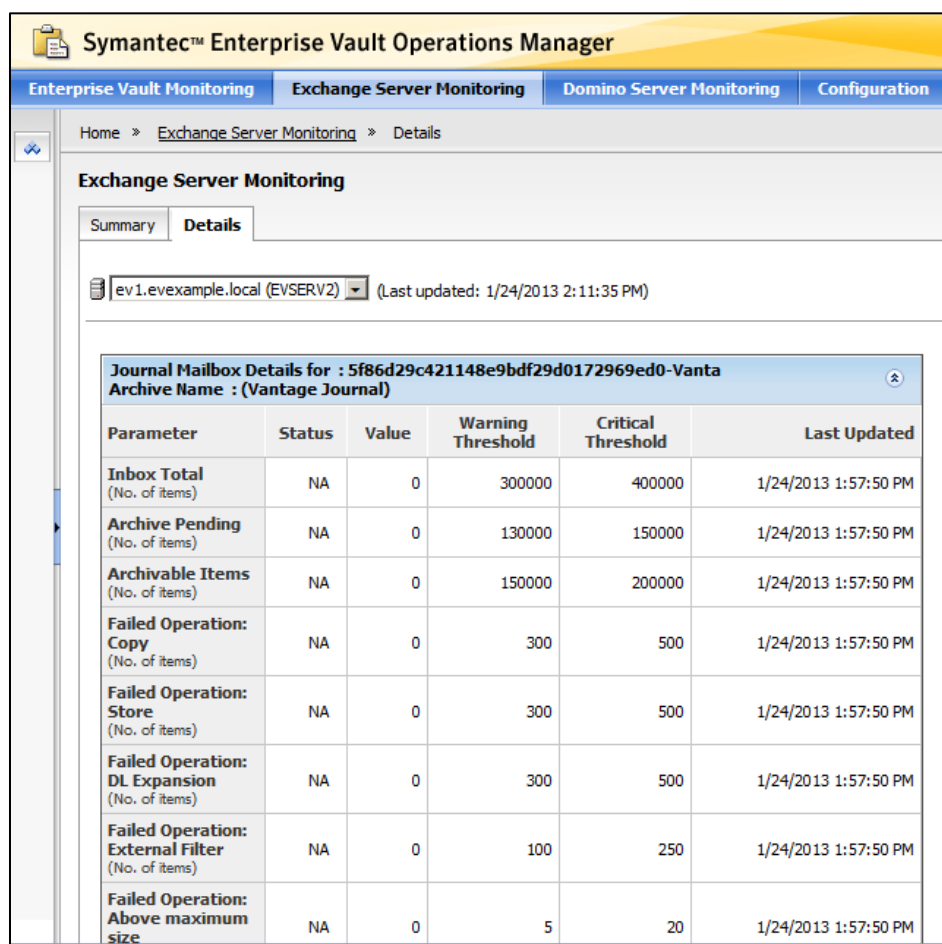


Figure 8 - Exchange Server Monitoring Details Page

Domino Server Monitoring

The Domino Server Monitoring tab is very similar to that of the Exchange Server Monitoring tab, but is specific to Domino journal archiving. The Details sub tab also provides more granular information on a selected Domino server and will provide journal archiving statistics over the past hour. As with Exchange Server Monitoring, if any of the monitored settings exceed the defined warning or critical thresholds, EVOM will change the status for the alert from Normal to either Warning or Critical.

The screenshot shows the Symantec Enterprise Vault Operations Manager interface. The main content area is titled "Domino Server Monitoring" and has a "Summary" tab selected. Below the tab is a table titled "Domino Server Journal Mailboxes : Overall Status". The table has the following columns: Server Name, Inbox Total, Archive Pending, Archivable Items, Failed Operations, Days Since Last Backup, and Last Updated. The data row shows the server "ev1.evexample.local (EVSERV2)" with green checkmark icons in the first five columns and a timestamp of "1/24/2013 2:10:25 PM" in the last column. Below the table is an "Icon Legend" section with three rows: a green checkmark for "Normal", a yellow warning triangle for "Warning", and a red X for "Critical".

Server Name	Inbox Total	Archive Pending	Archivable Items	Failed Operations	Days Since Last Backup	Last Updated
ev1.evexample.local (EVSERV2)	✓	✓	✓	✓	✓	1/24/2013 2:10:25 PM

Icon	Status
✓	Normal
⚠	Warning
✗	Critical

Figure 9 - Domino Server Monitoring Summary Page

Configuration

The Configuration tab allows the administrator to configure warning and critical thresholds for Enterprise Vault servers. The Performance Counters sub tab allows the administrator to set warning and critical thresholds for CPU, disk, memory, and general Enterprise Vault settings such as index operations, delete and restore operations, as well as backups of Enterprise Vault databases and vault stores. The administrator also has the ability to reset thresholds to default by clicking on the **Reset to factory** button. If any changes are made, the **Save** button must be clicked for the changes to take effect.

Operations Manager Configuration

Performance Counters Exchange Parameters Domino Parameters Monitoring Parameters



Configure Performance Counters		
Performance Counter	 Warning Threshold	 Critical Threshold
% Processor Time (%)	<input type="text" value="50"/>	<input type="text" value="90"/>
Available MBytes (MB)	<input type="text" value="50"/>	<input type="text" value="20"/>
% Free Space (%)	<input type="text" value="20"/>	<input type="text" value="10"/>
Number of incomplete backup, indexing or replication operations (No. of items)	<input type="text" value="500000"/>	<input type="text" value="2500000"/>
Number of incomplete delete operations (No. of items)	<input type="text" value="500000"/>	<input type="text" value="2500000"/>
Number of incomplete restore operations (No. of items)	<input type="text" value="1000"/>	<input type="text" value="5000"/>
Number of days since last backup of the vault store database (Days)	<input type="text" value="3"/>	<input type="text" value="15"/>
Space used in the vault store database transaction log (%)	<input type="text" value="85"/>	<input type="text" value="95"/>
Number of days since last backup of the vault store database transaction log (Days)	<input type="text" value="1"/>	<input type="text" value="5"/>
Cumulative size of all the log files in the database (KB)	<input type="text" value="85"/>	<input type="text" value="425"/>
Number of Saveset files awaiting backup or replication (No. of items)	<input type="text" value="5000"/>	<input type="text" value="25000"/>

Figure 10 - Configuration Tab

The Exchange Parameters and Domino Parameters sub tabs allow the administrator to configure warning and critical threshold levels for Exchange/Domino server monitoring. These thresholds are only valid if Exchange/Domino journaling is enabled. As with the Performance Counters, the administrator can reset all thresholds to default settings by clicking on the **Reset to factory** button. If changes are made, click on the **Save** button for the changes to take effect.

The Monitoring Parameters sub tab has three settings: Monitoring Enabled, Monitoring Frequency, and Retain Records For. The Monitoring Enabled checkbox can turn on or off monitoring for the selected Enterprise Vault site. The Monitoring Frequency setting determines how often (in minutes) that statistics will be collected. The default setting is 15 minutes. The Retain Records For setting determines how long collected data will reside in the Enterprise Vault Monitoring SQL database (the default is 30 days). The **Reset** button will reset all settings as set when the Monitoring Parameters sub tab was selected. For any changes to take effect, click on the **Save** button.

Home » Configuration » Monitoring Parameters Configuration

Operations Manager Configuration

Performance Counters Exchange Parameters Domino Parameters **Monitoring Parameters**

Configure Monitoring Parameters

Monitoring Enabled:	<input checked="" type="checkbox"/>
Monitoring Frequency (in minutes):	15
Retain Records For (in days):	30
Database Schema Version:	7.3.1.5

Reset Save

Figure 11 - Configuring Monitoring Parameters

For more information on Enterprise Vault Operations Manager, please review the Installing and Configuring guide specific to the version of Enterprise Vault running in the environment.

Enterprise Vault Reporting

Overview

Enterprise Vault Reporting uses Microsoft SQL Reporting Services to produce detailed reports for operations and File System Archiving. This feature was originally introduced with Enterprise Vault 7.0. Depending on how Microsoft SQL Reporting Services is configured, these reports can be emailed and saved to various formats such as PDF.

Enterprise Vault Reporting offers a different level of reporting compared to that of monitoring Enterprise Vault events recorded in the Windows log and EVOM. The administrator will be able to view reports specific to File System Archiving as well as Enterprise Vault Operations. File System Archiving reports are outside the scope of this document. An example of some of the operations reports include archive access, items archived per hour, Domino and Exchange journal reports, and vault store usage reports. These reports offer the administrator archiving trends as well as how much disk space is being used by archived content. Some reports will require additional Enterprise Vault components to be installed as detailed in the next section.

Installing and Configuring

Enterprise Vault Reporting is a separately installed component. To install, make sure that you are logged on as the Enterprise Vault service account (VSA). Insert the Enterprise Vault installation media and run Setup.exe from the Server folder. If all prerequisites have been installed (see below), Enterprise Vault Setup will offer the “Enterprise Vault Reporting” option.

The following prerequisites are required for Enterprise Vault Reporting:

- SQL Reporting Services must be installed using one of the following versions of SQL Reporting Services:
 - Microsoft SQL Server 2000 Reporting Services with SP2. IIS must be registered with ASP.NET 1.1. Enterprise Vault 9.0 no longer supports SQL Server 2000.
 - Microsoft SQL Server 2005 Reporting Services (SP1 or later recommended). IIS must be registered with ASP.NET 2.0.
 - Microsoft SQL Server 2008 Reporting Services. Enterprise Vault 8.0SP2 or later is required.
 - Microsoft SQL Server 2008 R2 Reporting Services. Enterprise Vault 9.0 or later is required.
 - Microsoft SQL Server 2012 x64 Reporting Services. Enterprise Vault 10.0.2 or later is required.
 - 64-bit versions of SQL Reporting Services (2005 and 2008) can be used; however, certain reports on vault store usage will not be available depending on the version of Enterprise Vault in use. These reports include the Vault Store usage reports. Enterprise Vault 9.0 and later no longer has these issues when using 64-bit versions of SQL Reporting Services.
 - For up to date information on SQL compatibility with Enterprise Vault, please refer to <http://www.symantec.com/docs/TECH38537>
- The Reporting Services component can be installed on a different server than the one containing the Enterprise Vault SQL databases.
- If installing Reporting Services on Windows 2008 Server, make sure that the IIS 6 Management Compatibility component is installed with Internet Information Services.
- There are additional prerequisites required for FSA Reporting which is outside the scope of this document. Please refer to the Installing and Configuring guide for your version of Enterprise Vault for more information.
- Some reports will require that monitoring be enabled. These reports include:
 - Enterprise Vault Server 24-hour Health Status
 - Enterprise Vault Server Seven Day Health Status
 - Exchange Server Journal Mailbox Archiving Health

- Exchange Server Journal Mailbox Archiving Trends
- Domino Server Journal Mailbox Archiving Health
- Domino Server Journal Mailbox Archiving Trends
- Some reports will require that auditing be enabled. This reports include:
 - Archived Item Access
 - Archived Item Access Trends
- Enterprise Vault Reporting also requires an Active Directory account in order to run under. It is recommended that this user be dedicated to reporting. The account does not need to have an email account set up nor does the account require any Windows administrative privileges. When configuring this user, make sure to set the account so that the password never expires. If using SQL 2000 Reporting Services, grant the account full access to the Temporary ASP.NET Files folder (by default located at C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322\Temporary ASP.NET files).
- Ensure that the Enterprise Vault service account (VSA) has the “Content manager” role assigned in Reporting Services. Please refer to Microsoft SQL Server Reporting Services documentation.
- Ensure that the Enterprise Vault service account (VSA) is added to the local administrators group on the Reporting Services server.
- At least one Enterprise Vault server needs to have had the Enterprise Vault Configuration wizard completed.

For detailed instructions on installing Enterprise Vault Reporting, please review the Installing and Configuring guide specific to your version of Enterprise Vault.

Accessing Enterprise Vault Reporting

To access Enterprise Vault Reporting, simply point a browser to the reports URL on the SQL Server Reporting Services server (e.g. <http://<ReportingServer>/Reports>). Once the web page comes up, a user will see a link for “Symantec Enterprise Vault”. Clicking on this will then present URL links to a language set to use (such as en-US). Once the language selected, two links will be presented, one for “Data Analysis Reports” and one for “Operation Reports”. Data Analysis Reports are for FSA Reporting and is outside the scope of this document. Operation Reports contains reports specific to Enterprise Vault operations. The number of type of reports will vary depending on which version of Enterprise Vault is installed.

The number of available reports will vary depending on the version of Enterprise Vault that is installed. For example, the Single Instance Storage reports will require Enterprise Vault 8.0 or later installed. For a complete list of available reports, please refer to the Enterprise Vault documentation specific to the version of Enterprise Vault in the environment.

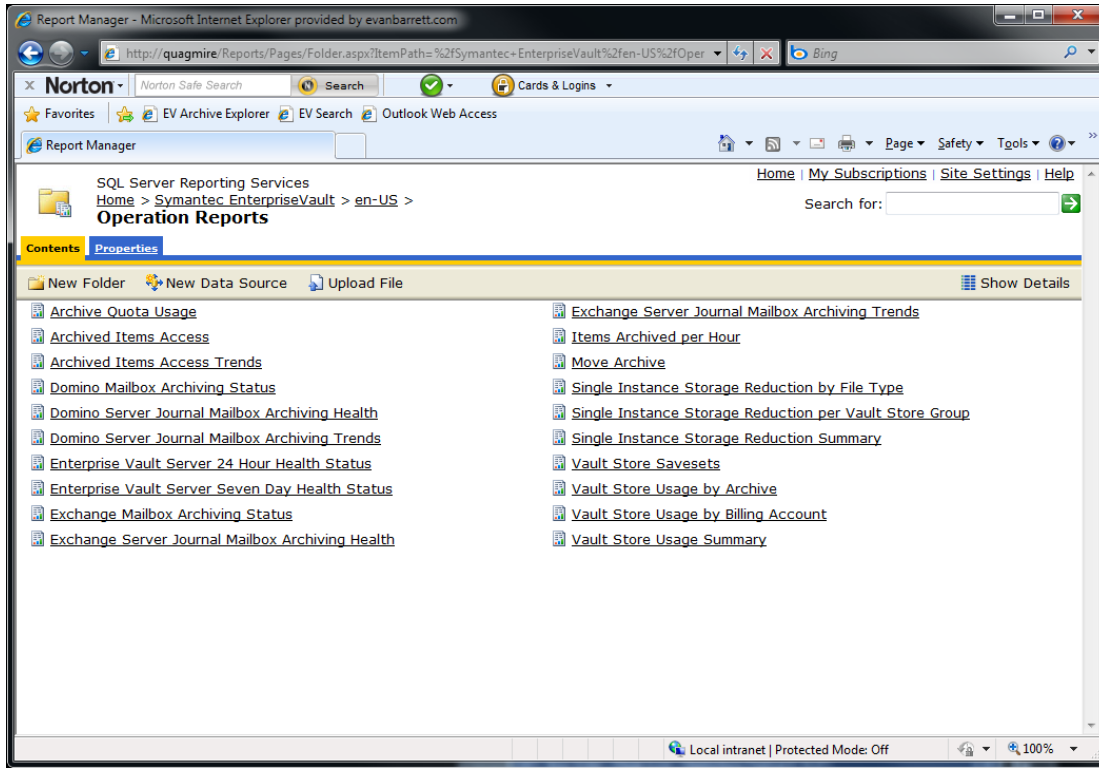


Figure 12 - Enterprise Vault Reporting Web Page

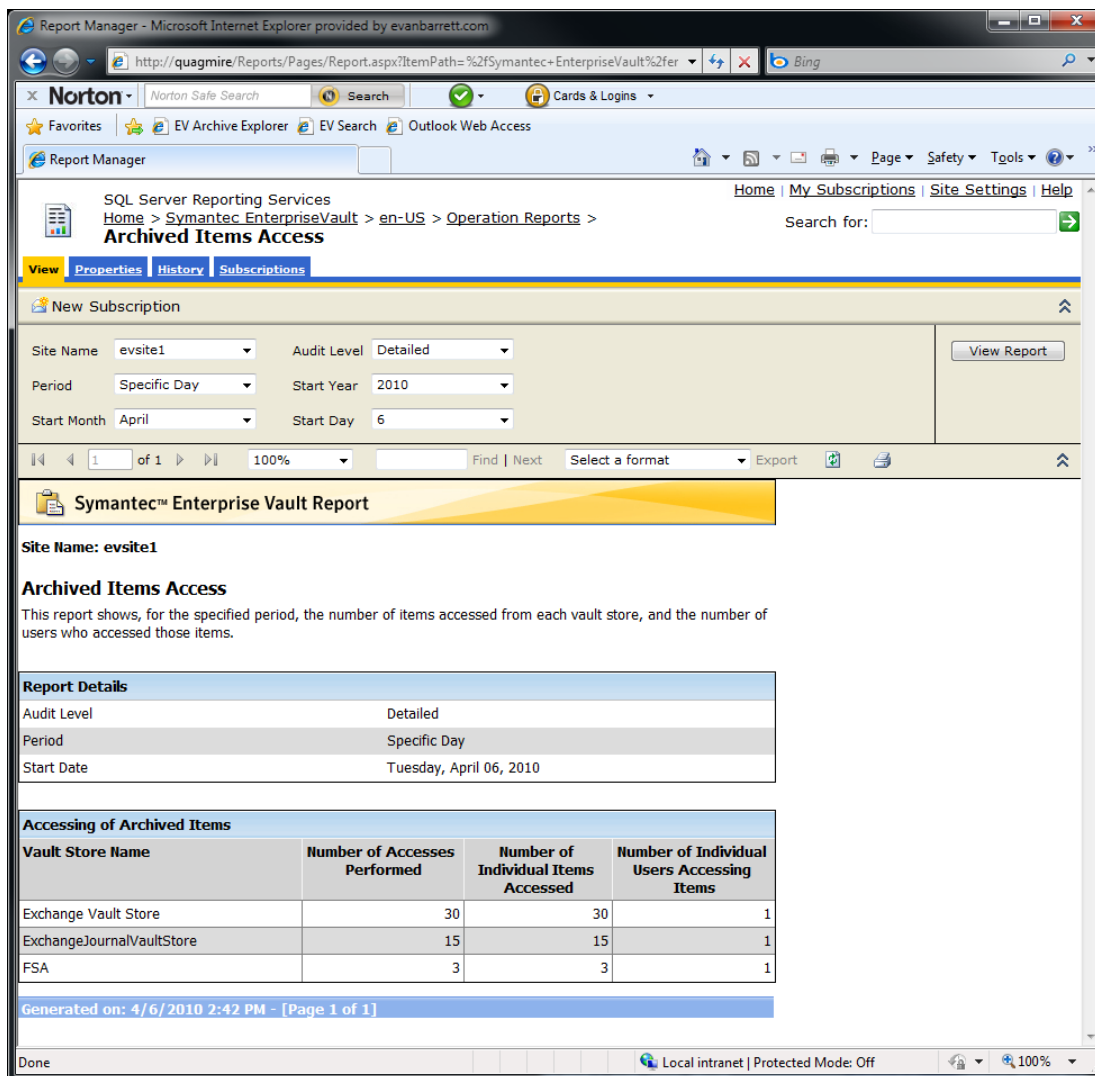


Figure 13 - Sample Archive Access Report

System Status

Overview

System Status, introduced with Enterprise Vault 8.0SP4, provides monitoring enhancements. The Enterprise Vault administrator or operator will more easily be able to identify any issues with Enterprise Vault every time the Enterprise Vault Administration Console is opened. The result is less time spent looking through Windows event logs and reports.

These enhancements include:

- Raises the visibility of monitoring alerts. The administrator or operator will no longer have to proactively scan the event logs. Only recent issues will be shown (and not the whole Event Log).

- A new container in the Enterprise Vault Administration Console (VAC) entitled “Status” is available (as shown in Figure 14)

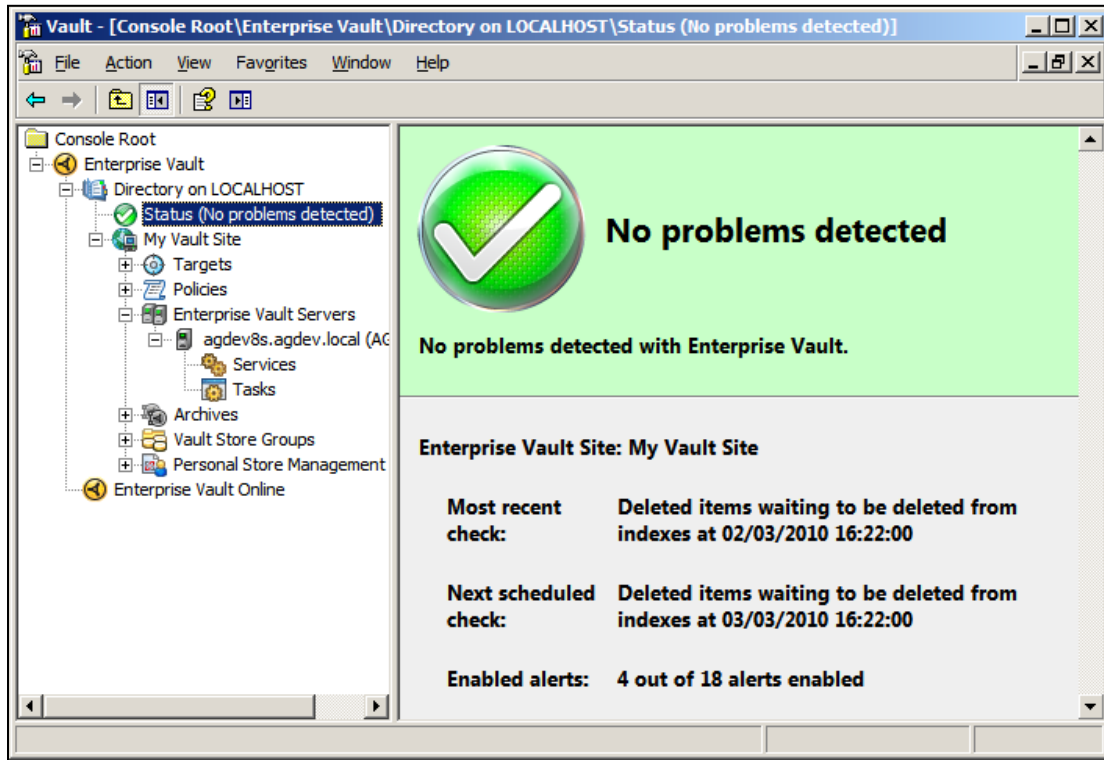


Figure 14 - System Status Overview

The icon for the Status container can change depending on the status (as shown in Figure 15).

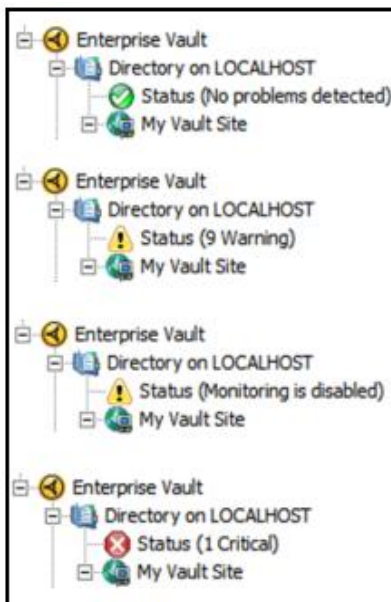


Figure 15 – System Status Examples

Installing and Configuring

System Status is installed automatically with Enterprise Vault 8.0SP4 or later. Microsoft .NET 3.5SP1 is also required to be installed on the Enterprise Vault server for System Status functionality within the Enterprise Vault Administration Console (VAC). Monitoring must also be enabled for the Enterprise Vault Site (please read the Enterprise Vault Operations Manager section of this document for more information).

Interacting with System Status

If there are alerts (Warning, Critical, or Error), System Status will provide details on the most recent alerts once the System Status container is selected in the VAC. Five columns are available: Severity, Alert name, Last Run time, Source of the alert, and the Enterprise Vault Site where the alert was triggered. The list of alerts can be sorted and reordered by clicking on the desired column. It should be noted that any severities listed in System Status will not necessarily be reported as an “Error” in the Windows event log.

Severity	Alert	Last Run	Source	Site
Critical	Vault Store fingerprint database backup	02/03/2010 17:34	Vault Store Group 1	My Vault Site
Critical	Vault Store fingerprint database backup	02/03/2010 17:34	Vault Store Group 2	My Vault Site
Critical	Vault Store fingerprint database log b...	02/03/2010 17:34	Vault Store Group 1	My Vault Site
Critical	Vault Store fingerprint database log b...	02/03/2010 17:34	Vault Store Group 2	My Vault Site
Critical	Vault Store in Backup Mode	02/03/2010 17:34	Enterprise Vault	My Vault Site
Critical	Vault Store partition backup scan	02/03/2010 17:34	Enterprise Vault	My Vault Site
Critical	Vault Store transaction log backup	02/03/2010 17:34	Vault Store 1	My Vault Site

Check for Vault Stores in backup mode		How to fix
One or more Vault Stores is in backup mode.		
Vault Stores in backup mode: 1 Total Vault Stores: 3		
Vault Stores in backup mode:		
Vault Store 2 in VSG1:END		
Items in mailboxes will remain in an archive-pending state.		
Example symptoms: archive-pending items remain in mailboxes, leading to calls to your Help Desk from users. New data cannot be archived. There may be Help Desk calls because		

Figure 16 - System Status List View of Recent Events

Details of an alert will be presented once an alert has been clicked. If applicable, a “How to fix” link will appear in the upper right-hand corner of alert details section. Clicking on this link will bring up the appropriate article in the local help file that will give more information on the cause and possible fixes for the alert.

Monitoring can be refreshed from the System Status container by clicking on the options in the MMC actions pane, by right-clicking on the system status node, or in the results grid:

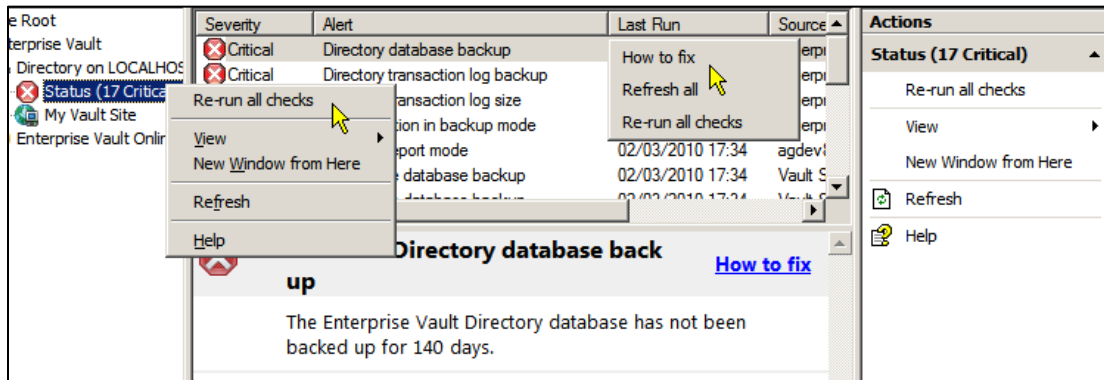


Figure 17 - Refreshing the System Status Display

When re-running all checks, alerts are refreshed for all Enterprise Vault sites that have monitoring enabled. This action is distributed across all Enterprise Vault servers in the environment and runs asynchronously. Because of the asynchronous operation, a window will appear providing a thirty second progress bar to give monitoring time to complete:

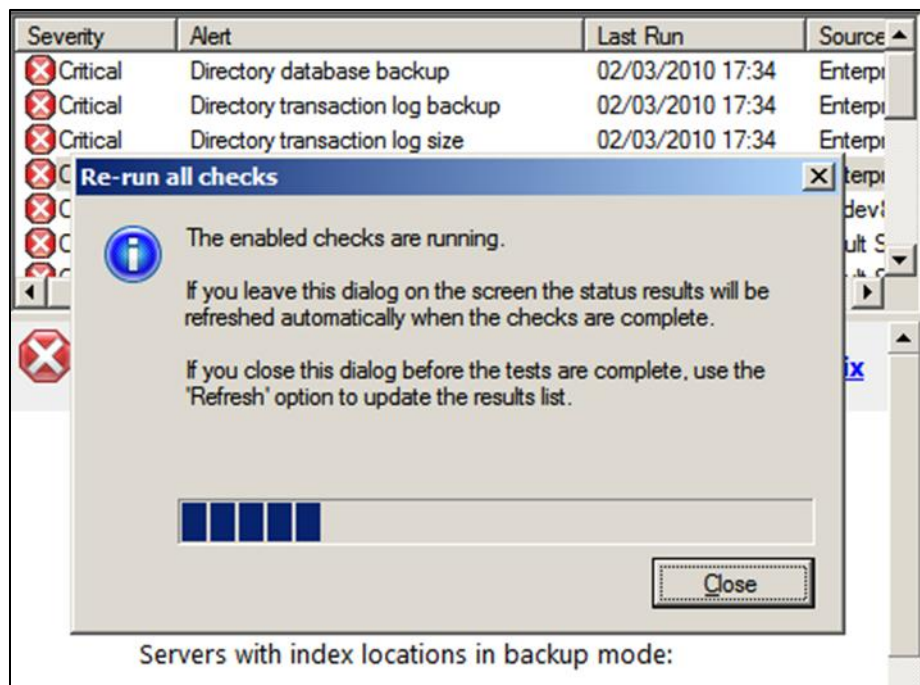


Figure 18 - Progress of System Status Refresh

Enterprise Vault Online

Enterprise Vault Online was introduced with Enterprise Vault 8.0SP4. This feature offers a container object in the Enterprise Vault Administration Console (VAC) that contains translated static HTML with URL links to Symantec support resources.

These commonly used HTML links are provided to make the job of researching support, compatibility, or service questions easier for the administrator or operator. The result is less time spent on finding where answers reside and getting the answers needed.

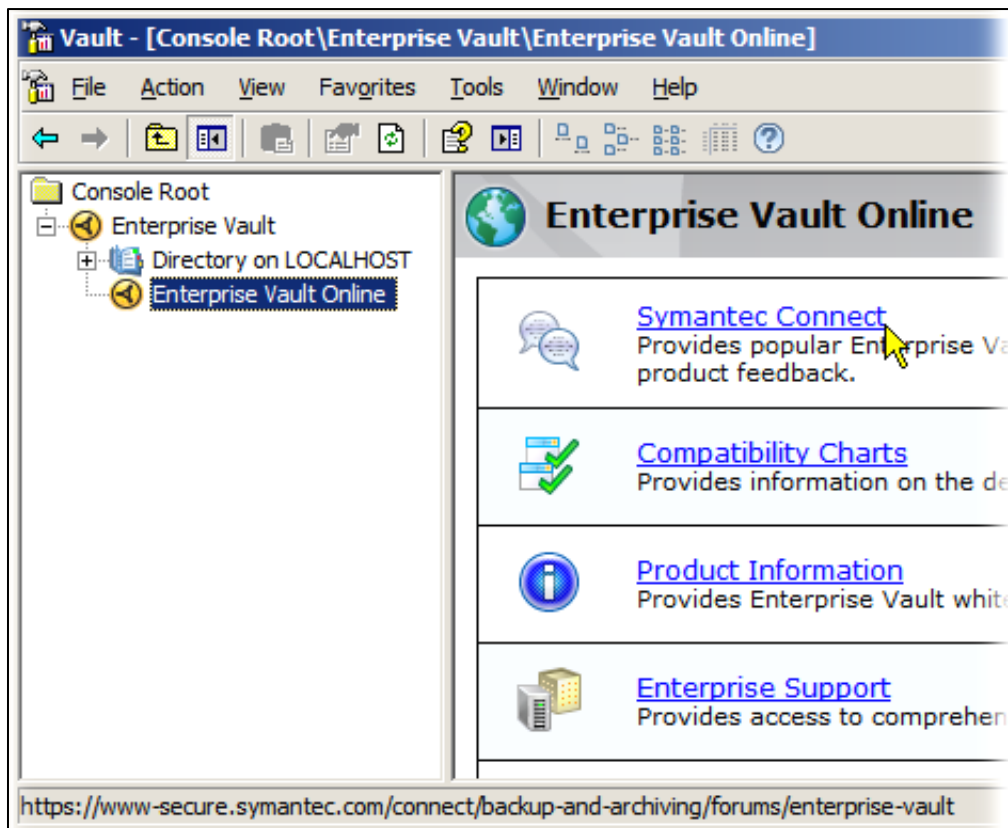


Figure 19 - Enterprise Vault Online Overview

The following are examples of items that can appear in the Enterprise Vault Online container. Additional items may appear depending on the version of Enterprise Vault being used.

- Symantec Connect – Provides popular Enterprise Vault discussion forums, articles, videos, blogs, and opportunities for product feedback.
- Compatibility Charts – Provides information on the devices and versions of the software that Enterprise Vault supports
- Product Information – Provides Enterprise Vault white papers and data sheets, articles, podcasts, and more.

- Enterprise Support – Provides access to a comprehensive knowledgebase and other support options for Enterprise Vault.
- MySupport Online Service Portal – Provides a means to submit and manage Enterprise Vault support cases.
- Email Bulletin Service – Provides free Technical Support bulletins to keep you informed about product updates and download, the latest offerings from Technical Support, and tips and tricks.
- Symantec Global Services – Provides access to expert resources for deploying, managing, and supporting Symantec products
- Find a Symantec Partner – Provides resources for locating Symantec partners who can deliver products, solutions, and services in your region.
- Doing Business with Symantec – Provides a quick way to find answers to common questions about doing business with Symantec, and links to more information and contacts.

Monitoring Using Microsoft Operations Manager

Overview

Microsoft Operations Manager (or MOM) is a software package from Microsoft that performs datacenter monitoring on the following items:

- Event-driven operations monitoring
- Performance tracking
- Security policy enforcement
- Audit capabilities

For more detailed information on MOM, please visit <http://technet.microsoft.com/en-us/systemcenter/bb498244.aspx>.

Enterprise Vault is shipped with ability to work with Microsoft Operations Manager. The Enterprise Vault Management Pack contains rules that enable MOM to monitor critical Enterprise Vault events in the Application Event Log. MOM can also monitor all alerts that have been configured in the Monitoring tab in the Site Properties. Alerts defined in the Monitoring tab are written as critical events to the event log. By default, MOM will pick up these critical events.

Installing and Configuring

Microsoft Operations Manager must already be installed and configured before performing integration with Enterprise Vault. Please review MOM documentation on how to install and configure MOM.

The MOM Management Pack can be found in the MOM subfolder of the Enterprise Vault installation folder (by default C:\Program Files\Enterprise Vault\MOM). The name of the file containing the Management Pack is EnterpriseVault.akm.

To enable MOM monitoring of Enterprise Vault, perform the following tasks:

- 1) Start the MOM Administrator Console
- 2) In the left pane, right-click Processing Rule Groups and select Import Management Pack from the shortcut menu.
- 3) Select the Enterprise Vault Management Pack file and finish the Import Options wizard
- 4) To add operators to the Enterprise Vault notifications group:
 - a. In the MOM Administrator Console, expand Rule Groups,
 - b. Click Notification Groups
 - c. In the right pane, double-click Enterprise Vault Administrators
 - d. Add the operators who should receive alerts
 - e. Click OK

Optional Configuration

The Enterprise Vault MOM Management Pack defines many rules for Enterprise Vault monitoring, some of which are enabled by default and some of which are disabled. Review the rules and enable or disable as required.

When the Enterprise Vault administrator has configured the Enterprise Vault MOM management pack, it may be necessary to configure some of the rules before they can be used.

For example, if an administrator wants to use the following rule, it must be configured to specify which SQL server to monitor:

Sample value of the performance counter SQL Server - Checkpoint pages

/ sec is greater than the defined threshold

Note that some MOM rules concern events that are themselves enabled by the Enterprise Vault Administration Console. In the case of these events, they must be enabled in the Administration Console.

For a complete list of MOM rules and corresponding events, please review the Enterprise Vault Administrators Guide for the version of Enterprise Vault in the environment.

Monitoring Using System Center Operations Manager 2007 and 2012

Overview

Enterprise Vault 10.0.2 and Earlier

System Center Operations Manager 2007 (or SCOM) is a software package from Microsoft that replaced Microsoft Operations Manager 2005. For more information on SCOM, please visit <http://www.microsoft.com/systemcenter/en/us/operations-manager/om-overview.aspx>

Enterprise Vault includes a management pack for System Center Operations Manager 2007 (SCOM). This management pack includes rules that enable SCOM to monitor critical Enterprise Vault events in the Application Event Log. SCOM can also monitor all the alerts that have been enabled for a site as defined in the Monitoring tab in Site Properties. Alerts defined in the Monitoring tab are written as critical events to the event log. By default, SCOM will pick up these critical events.

Enterprise Vault 10.0.3 and Later

Starting with Enterprise Vault 10.0.3, a new SCOM management pack is available which will allow administrators to monitor Enterprise Vault internal objects such as sites, servers, services, tasks, dependency services, etc. The SCOM management pack introduces a new structured hierarchy for Enterprise Vault in SCOM this enables operators to view any alerts or check the status of the system by logical components. In order to use the newer SCOM management pack, the following conditions must be met:

- The Enterprise Vault server must have PowerShell 2.0 installed
- SCOM Server 2007 R2 or SCOM Server 2012
- The SCOM agent must be installed on the Enterprise Vault server

The SCOM management pack introduced with Enterprise Vault 10.0.3 will work with older versions of Enterprise Vault (9.0 through 10.0.2). However, these versions of Enterprise Vault will be limited to alerting only (service and task monitoring is available for EV 10.0.3 and later). If an older version of the SCOM management pack is being used, it must be uninstalled first before installing the EV 10.0.3 (or later) version of the management pack.

More information on the 10.0.3 (and later) SCOM management pack can be found in the Enterprise Vault 10.0.3 (and later) Administrator's Guide.

Installing and Configuring – Enterprise Vault 10.0.2 and Earlier

System Center Operations Manager 2007 (SCOM) must be installed and configured before performing integration with Enterprise Vault. Please review the SCOM documentation on how to install and configure SCOM.

The SCOM Management Pack can be found in the SCOM subfolder of the Enterprise Vault installation folder (by default C:\Program Files\Enterprise Vault\SCOM). The name of the Management Pack file is EnterpriseVault.xml.

To enable SCOM monitoring of Enterprise Vault, perform the following steps:

- 1) Use the SCOM management console to add the SCOM monitoring agent to the Enterprise Vault server so that the server is Agent Managed.
 - a. Start the import wizard and import the EnterpriseVault.xml file from the SCOM folder on the Enterprise Vault server.
 - b. The wizard will convert the file to a MOM 2005 Backward Compatibility pack.
- 2) Ensure that monitoring is enabled for each site to be monitored
 - a. Right-clicking on the Enterprise Vault Site name and bring up Properties
 - b. Click on the Monitoring tab
 - c. Ensure that the site is being monitored. Select all or any alerts that will be monitored.
- 3) In the SCOM management console, review the Enterprise Vault alerts and modify as required

Optional Configuration (Enterprise Vault 10.0.2 and Earlier)

The Enterprise Vault SCOM Management Pack defines many rules for Enterprise Vault monitoring, some of which are enabled by default and some of which are disabled. Review the rules and enable or disable as required.

When you have configured your Enterprise Vault SCOM management pack, you may need to configure some of the rules before you can use them.

For example, if you want to use the following rule you must configure it to specify which SQL server to monitor:

Sample value of the performance counter SQL Server - Checkpoint pages

/ sec is greater than the defined threshold

Note that some SCOM rules concern events that are themselves enabled by the Enterprise Vault Administration Console provided that they have been enabled.

In Conclusion

Enterprise Vault services and tasks utilize the Windows event log to record events that take place in an Enterprise Vault environment. Proactive monitoring of these events is the first line of defense in preventing and determining any issues that may exist.

There are additional components available to assist with monitoring Enterprise Vault. Depending on what version of Enterprise Vault is installed, one or more of these features may be able: Enterprise Vault Operations Manager (EVOM) and System Status. EVOM is a web-based utility that will quickly present the overall status of Enterprise Vault environment providing information on Enterprise Vault server health (such as CPU, memory, and disk space utilization), current service and task status, and the status of journal mailbox archiving for Microsoft Exchange and Lotus Domino. System Status provides a view of the status of Enterprise Vault environment using the Enterprise Vault Administration Console. It can also provide solutions to any potential issues by providing links to various Enterprise Vault help files. As a side note, Enterprise Vault Online (available in the Enterprise Vault Administration Console), introduced with Enterprise Vault 8.0SP4, presents commonly accessed HTML links to information related to support, compatibility, and services.

Third party monitoring utilities, such as Microsoft SCOM Server, can provide centralized monitoring of an Enterprise Vault environment. Starting with Enterprise Vault 10.0.3, the SCOM management pack provides additional reporting on all aspects of Enterprise Vault.

About Symantec:

Symantec is a global leader in providing storage, security and systems management solutions to help consumers and organizations secure and manage their information-driven world.

Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site: www.symantec.com

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934

Copyright © 2013 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.