WHITE PAPER: DATA AND SYSTEM PROTECTION

Symantec Enterprise Vault™

Enterprise-Scale Administration

Steven Buccola
January 4, 2007

White Paper: Data and System Protection

Symantec Enterprise Vault
Enterprise-Scale Administration

Contents

Introduction to Enterprise-Scale Administration

Over the past few years, archiving has quickly moved beyond its role as the pet project of the Microsoft® Exchange administrator for reducing Exchange storage. It has fast become an integral part of the information lifecycle strategy of companies, allowing them to define where enterprise data is stored and for how long. With access to electronic data expanding beyond IT administrators to legal teams, human resources staff, and temporary project teams, archiving can actually be a corporate asset. And more and more archiving policies are being developed based on users' roles, as awareness increases for the technical capabilities of applications like the Symantec Enterprise Vault framework.

Given this rise in the importance of archiving solutions, administrators are being tasked to:

- Easily tailor archiving policies for a workforce dealing with diverse end-user requirements.

  Granular policies can be assigned to a wide variety of users' mailboxes and PST files, harnessing Active Directory® groups and queries, and automatically synchronized via the Enterprise Vault *provisioning* facility. Custom mailbox folder-level policies can further define custom retention periods as well as create immediate archiving rules for special uses such as a zero-day archive on a user's Sent Items folder.

- Place more controls on how users' information is managed and accessed, and reduce management costs by distributing administrative responsibilities across large IT teams.

  Enterprise Vault addresses the need to distribute administrative access and functions to many types of system administrators with its *roles-based administration* functionality, which delegates administrative authority by Active Directory users and/or groups.

- Provide informative reports about the status and trends in the archive.

  For those seeking insight into their archive system's health and trends, the Enterprise Vault *operations monitoring and reporting* platform is a valuable resource.

All of these components are built into the core Enterprise Vault product, requiring no additional licensing and only minimal additional configuration.

This white paper reviews each of these Enterprise-Scale Administration features from Symantec, providing a basic understanding of how these solutions can be configured and utilized.

Granular policies and provisioning

Enterprise Vault offers granular policy management, so administrators can easily and automatically enable tailored mailbox archiving policies for both new and existing Exchange users. Enterprise Vault provisioning lets administrators identify users who require unique archiving settings—such as terminated employees or VIP individuals—and give them archiving and retention policies that are distinct from the majority of the user population. Users of Mac or laptop systems may need unique client settings, because of the capabilities of their mail client and the way it is used. The granular policies and provisioning features also make it possible to efficiently scale a large archiving implementation, dividing the user population evenly across multiple Enterprise Vault servers and storage devices.

Management of the granular policies, as with most Enterprise Vault functionality, is found within a central Administration Console, which is a convenient snap-in to the Microsoft Management Console (MMC). From this central console, Enterprise Vault administrators can easily manage all Enterprise Vault policies and servers, including servers located at remote sites.

Archiving policies

Policies allow an administrator to control several different areas of a user's mailbox environment, as well as how the user searches and accesses the archive from built-in Enterprise Vault applications.

There is a special Policies container in the Enterprise Vault Administration Console, with subcontainers for the various types of content that can be archived (see Figure 1). Although granular policies can be created and applied to many types of archiving sources, such as Lotus Domino®, Windows® file systems, and Microsoft SharePoint®, this white paper addresses Microsoft Exchange only.

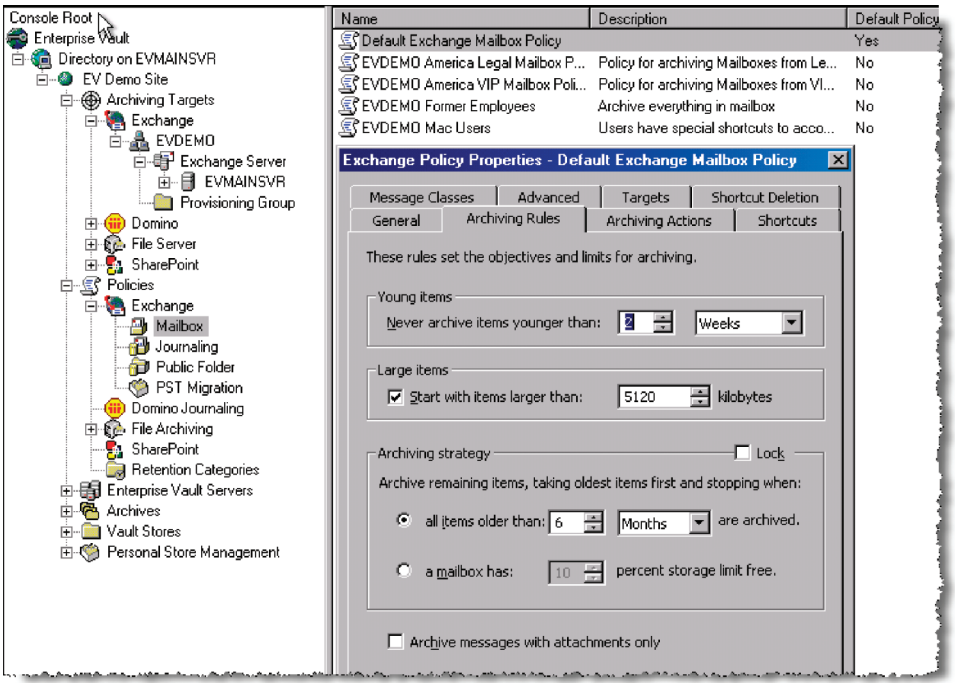


Figure 1. Sample Exchange mailbox archiving policy.

Exchange archiving policies can control several aspects of the archiving process and end-user experience, such as:

- **Archiving strategy.** Includes parameters such as when email will be automatically archived (based on size, age, or user's proximity to Exchange mailbox quota) and whether certain message classes will be archived from the mailboxes.
- **Shortcuts.** Includes the number of characters that should be stored in the shortcut body text, optional hypertext links to download the whole message or specific attachments, and the length of time shortcuts reside in the mailboxes before automatic deletion.
- **Client behavior.** Enables, disables, and configures certain end-user features such as Offline Vault, Outlook Web Access, Archive Explorer, search applications, manual archive and restore functionality, and more.
- **PST migration.** Specifies whether PSTs are deleted after migration, whether shortcuts to migrated items are created in the users' mailboxes, and more.

There are no limits to the number of policies that can be created, and a policy need not be assigned to only one user or group. All policies are available for all mailboxes that are archived within the same logical Enterprise Vault site.

Once a policy is chosen and provisioned to one or more mailboxes (as described in the "Provisioning Groups" section), the effects of the archiving policies can be projected by running the Exchange Server's Archiving Task in Report Mode. This process does not modify any content in Exchange or archive any new data to Enterprise Vault. Instead, it tests the policy against the Exchange Server(s) and generates a tab-delimited text file detailing:

- which mailboxes would be archived
- the number of messages to be archived and their average size
- the projected size of the mailbox post-archiving

Refer to the "Archiving Simulation Reports" section for more information.

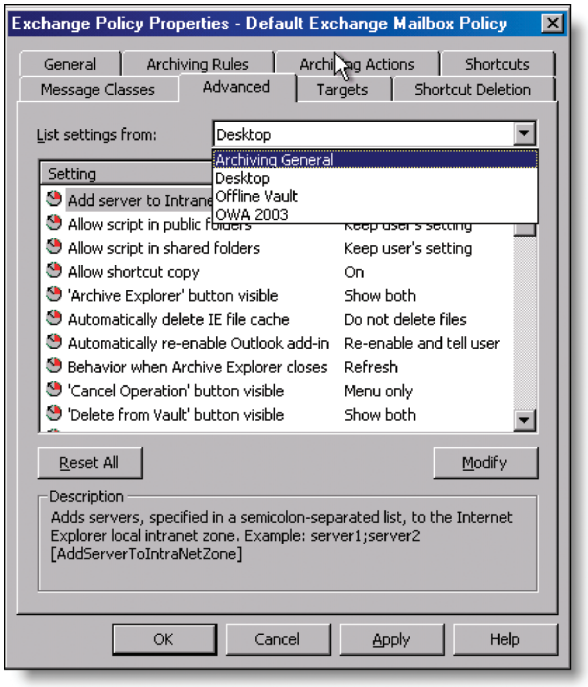


Figure 2. In Advanced Setting, the end user's interaction with archived content can be modified.

There are more than 100 options and controls available within an Exchange Mailbox Policy (see Figure 2); refer to the *Enterprise Vault Administrator's Guide* for more detailed information on specific policy functionality.

Provisioning groups

Once mailbox archiving policies are defined, they are assigned to mailboxes through the use of Provisioning Groups. A provisioning group is a set of mailboxes which Enterprise Vault determines through Active Directory queries. These mailboxes can be selected from Active Directory by specifying from the Enterprise Vault admin console any of the following:

- Windows user
- Windows Security Group
- Windows Distribution Group
- Organizational Unit
- LDAP query
- All mailboxes in an Active Directory domain

Note: For users belonging to more than one Security or Distribution Group, the Provisioning Task assigns a policy to the first matching group in which it encounters the user.

As an archiving target, provisioning groups are logically found in the Administration Console under each Active Directory domain. Provisioning groups are created after the archiving policies, as the properties of each provisioning group contain an Exchange Mailbox Archiving policy, PST migration policy, and Retention policy that should be applied to the group's members.

In addition to assigning archiving policies to specific users, administrators can use provisioning groups to scale the archive for large numbers of users and large volumes of data by specifying particular vault stores and indexing services for certain groups of users (see Figure 3). Example 2 in the next section describes the structuring of groups.

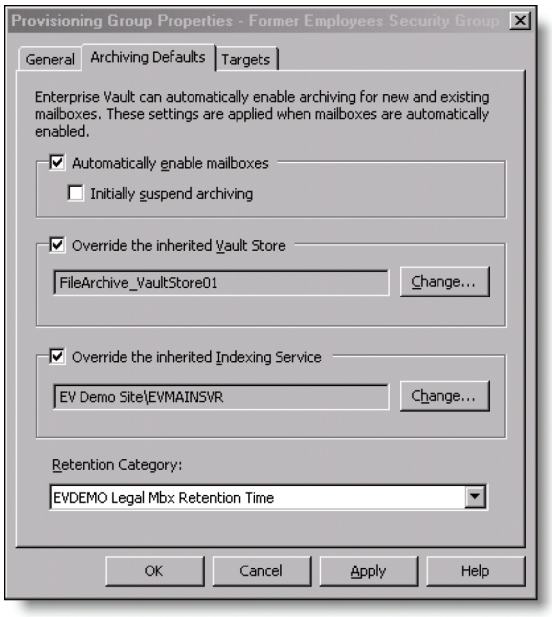


Figure 3. Provisioning group properties, which affect how mailboxes are processed by specifying alternative servers and storage devices.

Since mailboxes can be members of multiple Active Directory security and distribution groups, the order in which provisioning groups are listed in the Administration Console resolves any conflict caused by being a member of multiple groups. Provisioning groups are processed from those ranked first in the list to those placed last. Mailboxes that appear in more than one group use the settings from the first group in which they appear. Therefore, employees with the most specific archiving requirements should be placed higher in the list than those belonging to a broader class of archiving needs.

If a user's Active Directory membership changes to a provisioning group of higher priority, the Provisioning Task moves the mailbox to the new provisioning group once synchronization with the task and Active Directory occurs. The mailbox is then archived according to the policies of the new group.

The broadest provisioning group would consist of all Exchange mailboxes in a particular Active Directory domain. In this case, it is recommended that the provisioning group be created for the entire domain at the bottom of the list, as shown in Figure 4.

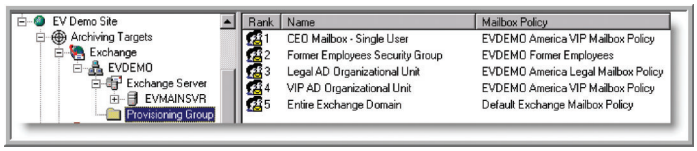


Figure 4. Provisioning groups within the Enterprise Vault Administration Console.

In addition to the set of groups displayed in this provisioning group container, an associated Provisioning Task for each domain synchronizes user membership between each provisioning group and Active Directory. This task can be scheduled to run up to twice a day, and can also be run manually by the administrator at any time.

The process by which mailboxes are enabled for archiving is as follows:

1. **Provisioning Task is created.** A Provisioning Task must exist for each domain hosting Exchange mailboxes to be archived.
2. **One or more provisioning groups are created.** Each mailbox must match at least one provisioning group before it can be archived.
3. **Provisioning Task is run.** This assigns the appropriate policies to the appropriate mailboxes. The task automatically runs twice a day, but can be run manually as well.
4. **Mailboxes are enabled for archiving.** This can be done automatically via the Provisioning Task, or manually via a wizard-driven process. This step instructs the Enterprise Vault to include the specified mailboxes in subsequent runs of the Archive Task, following the archiving policies assigned to them. A PST migration policy is also assigned to the user's mailbox at this time.
5. **Archive Task is scheduled to archive the enabled mailboxes.** The mailboxes are archived at the scheduled interval designated by the administrator on a per–Exchange Server basis.

Example scenarios for granular policies and provisioning groups

There are countless usage scenarios for granular policies and provisioning; for instance, one might want to assign:

- Heavy email users with a shorter shortcut deletion policy than their peers
- The legal department with a longer retention policy than the rest of the organization
- The mobile sales force with an automated Offline Vault installation for their offline use

- Former employees with a zero-day archive policy to capture all content in their mailboxes
- Special vault storage devices for particular groups of users, such as executives or regulated employees

Here we explore two such scenarios in detail.

Example 1—Archive all content from former employee mailboxes

In today's dynamic business world, employee turnover is inevitable, so handling information from former employees is an ongoing and tedious task for system administrators. Because Exchange mailboxes are often the most comprehensive source of historical information about an employee's projects, customer interactions, and commitments, most organizations choose not to immediately delete the content from Exchange mailboxes when an employee leaves the company.

Rather than preserve this dormant mailbox and content within the Microsoft Exchange primary storage, the Enterprise Vault administrator could be more efficient by following a process like the following:

1. Create a Windows Security or Distribution group with a clear name such as Former Employees Group.
2. Create an Enterprise Vault Exchange Mailbox Archiving policy with a clear name such as Former Employees Mailbox Policy, which contains the following settings:
   - Never archive items younger than: 0 days
   - Archive items older than: 0 days
   - All message classes selected [Ideally, add a custom class with a wildcard (*).]
   - Do not create shortcut to archived item
   - Delete original item after archiving
   - Archive unread items
3. If applicable, create an Enterprise Vault PST migration policy—with a name like Former Employees PST Policy—with the following settings:
   - Do not create shortcuts for imported items
   - Delete PST file when migration is complete
   - Do not restrict file search to Documents & Settings profile folder
   - Migrate the "Deleted Items" folder
   - Archive non-expired calendar items

4. Create a new provisioning group called Archived Former Employees. Specify Former Employees Group as its membership, then specify the Former Employees Mailbox Policy and Former Employees PST Policy for this group.

5. Place this new provisioning group very high, if not at the top, in the order of groups, as many of these mailboxes may also be members of other groups and distribution lists with far less aggressive archiving and PST migration policies.

Example 2—Assign storage devices by group

Aside from controlling how users interact with the archive via an Archive Policy, provisioning groups can also help administrators scale and structure which mailboxes will be processed by the Enterprise Vault servers, and where the mailboxes' archived data will be stored.

Enterprise Vault supports an unparalleled number of storage devices for archive content, ranging from "tier 1" block-level storage devices like storage area networks (SANs) to a variety of lower-cost file-level or content-addressable storage (CAS) devices—and even common tertiary storage media such as tape—through direct product integrations with storage products such as Veritas NetBackup™.

With all these options to choose from, and to meet regulatory requirements such as storing content from certain individuals on nonerasable storage technology, it is common for medium to large organizations to scale the archive implementation using multiple types of storage devices, as business requirements dictate.

For example, an organization may wish to permanently store executive archives on the most high-performing, highly available storage technology, but keep the remaining archives on lower-cost, tiered storage. The process in this example would be as follows:

1. Create a vault store called Executive Store. Then create at least one vault store partition, using the most advanced storage technology available. (In the case of a SAN, the path for the partition would likely be represented in the form of a directly attached drive letter and path, such as S:\Exec_Storage\.)

2. Create another vault store called Default Vault Store. Create at least one vault store partition, using lower-cost storage technology this time. (If using a NAS, the path will likely be entered as a UNC path, such as \\nasdevice\sharename. Content-addressable storage (CAS) devices are often configured by one or more IP addresses.) If appropriate, configure the Default Vault Store to migrate archived content from the primary vault store partition to a second location when it reaches a certain age. This is a popular way to reduce total cost of ownership (TCO) for the

archive even more significantly over time, but may not be appropriate for certain users, such as the executives in this example.

3. Now create a Windows security or distribution group called Executive Mailboxes, and configure its membership to include all executives who require the fastest and most highly available storage. Alternatively, organize all executive user objects into a common Organizational Unit (OU) with a clear name that can later be referenced by the Enterprise Vault provisioning group.

4. Create an Enterprise Vault provisioning group called Executive Archives, specify the Windows group or OU as configured in the previous step for the membership of this provisioning group; specify the appropriate archiving, PST migration, and retention policies for the executive mailboxes; and specify the vault store called Executive Store for members of this group.

5. Arrange this new group very high, if not at the top, in the provisioning group order, in case the executives also belong to other provisioning groups with more standard policies.

Folder-level policy granularity with Enterprise Vault Policy Manager

Further customization of a user's mailbox archiving policy can be accomplished using a special utility called Enterprise Vault Policy Manager. This command-line tool can be used in addition to, or instead of, the granular policies and provisioning groups previously discussed. From the command line, the administrator executes a plain-text policy definition file that contains specific instructions on how certain mailboxes should be processed. Unlike provisioning groups, the Enterprise Vault Policy Manager utility can specify folder-specific archiving policies such as:

- Create a custom folder called Legal Retention that is archived after zero days and applies a retention policy for 99 years.
- Create a whole series of standard mailbox folders, each assigned unique retention policies, according to the organization's electronic content retention policy.
- Specify a 3-day archiving policy and 30-day shortcut retention for the Deleted Items folder.
- Specify a 7-day archiving policy and 6-month shortcut retention for the Sent Items folder
- Specify a 2-week archiving policy for past calendar appointments and leave no shortcuts.
- Assign a set of Windows users and/or groups permissions to a specific archive for a shared project

If provisioning groups are being used to enable users with a broad-based policy, Enterprise Vault Policy Manager can be valuable in refining the archiving instructions to an even more granular level, without impeding other policies. All mailbox folders would, by default, inherit the archiving policies specified in the mailbox's provisioning group, unless specifically overridden by the Enterprise Vault Policy Manager utility.

The **Vault Service Account (VSA)** can perform all Enterprise Vault management operations with no restrictions. Initially, the VSA is the only account that can create roles and assign them to lower-level administrators.

Roles-based administration

As organizations grow and IT teams specialize in application and hardware tiers, there are increasing demands for enterprise-class software to provide granular security control to portions of the product. As an enterprise-wide platform for content archiving, Enterprise Vault is often administered by many diverse and, at times, disparate individuals and teams. These administrators may need only limited access to manage their own part of the application, for security reasons and to limit liability and risk to the fewest individuals.

For instance, network administrators may need to manage and archive their own file servers, without being exposed to email archiving objects and functions. Or there may be a separate storage team with archive storage access only for backups, while the desktop team should only be able to enable users for mailbox archiving. And in a distributed environment, local teams may need to narrow their focus to only their own Enterprise Vault site.

Enterprise Vault provides roles-based administration just for this purpose. First, it creates a set of roles for grouped functions of the product (e.g., File Administrator role for file archiving functions); next, it allows administrators to modify the defined roles as needed; and finally, it allows an administrator to specify which other users or groups belong to the various roles. With these capabilities, Enterprise Vault administrators no longer need to share a single Vault Service Account and password with complete administrative rights to the entire archiving platform.

Role definition

Enterprise Vault leverages the Microsoft Authorization Manager MMC span-in to harness its unique Active Directory integration methodology to structure a set of roles, each allowing access to specified operations and tasks. These roles are not set up initially, but are created by the initial user who is setting up Enterprise Vault and logged into Windows with the Vault Service Account credentials. This person specifies the users and groups to whom access can be delegated.

Within Authorization Manager, administrative roles are created and modified using operations and tasks:

- An *operation* is a low-level permission that represents a privileged action or capability. When the Administration Console determines whether a role has access to perform a task, it is the operations associated with the role that are checked.
- A *task* is a group of operations that collectively provide sufficient permissions to do a particular job.
- An administrative *role* is a collection of tasks, and possibly operations and other roles.

Enterprise Vault supplies the following predefined roles:

- **Messaging administrator.** Responsible for the day-to-day administration of Exchange archiving and Lotus Domino archiving. This administrator does not have access to other parts of the product, such as File Server archiving or SharePoint archiving.
- **File server administrator.** Manages file server archiving functions. This individual or group does not have access to other parts of the product, such as Exchange Server archiving or SharePoint archiving (see Figure 5).
- **PST administrator.** Configures PST migration policies and tasks, and can also monitor the progress of PST migration from the Personal Store Management container.
- **SharePoint administrator.** Configures SharePoint targets, policies, and tasks.
- **Storage administrator.** Manages all components needed to keep Enterprise Vault storage running properly, including vault stores and partitions, archive properties, and matching archiving targets to appropriate vault stores. There is no access to archiving policies.
- **Power administrator.** Performs all the tasks in the other predefined roles. Cannot perform significant reconfiguration tasks such as changing the Vault Service Account or Directory SQL Server (these tasks can only be done using the VSA).

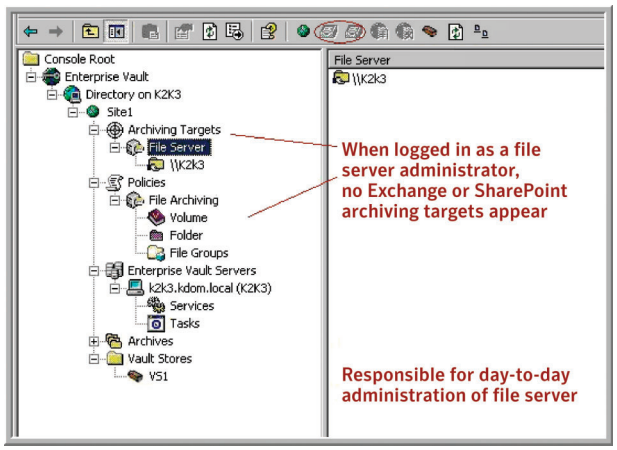


Figure 5. The File server administrator manages file server archiving functions.

It is possible to use the predefined roles as supplied, customize them, or create new roles as required.

By assigning administrator roles, you can adjust the permissions of individual administrators to match their job responsibilities. The mechanism is flexible enough to modify an individual's role to cope with any change in responsibility.

Role assignments

You can assign administrator roles to the following (see Figure 6):

- Windows Users and Groups.
- The results of an LDAP query.
- Application-specific groups. These groups, specific to Authorization Manager, can contain a mixture of users and groups. They can also be based on an LDAP query. The main benefit of using application groups is that there is no need to create new groups within Active Directory to support Enterprise Vault.

Figure 6. Assigning users and groups to a role.

By default, an administrator in any given role has access to all Administration Console containers relevant to that role. For example, a Messaging Administrator has access to every Exchange Server and Domino server in the Enterprise Vault Site. However, administrator access permissions can be granted or denied on individual containers in the Administration Console, so you could, for instance, grant a person access to administer archiving for only a specific Exchange Server (see Figure 7).

Access permissions can be granted or denied on any of the following containers:

- A file server
- An Exchange Server
- A SharePoint virtual server
- An Enterprise Vault server

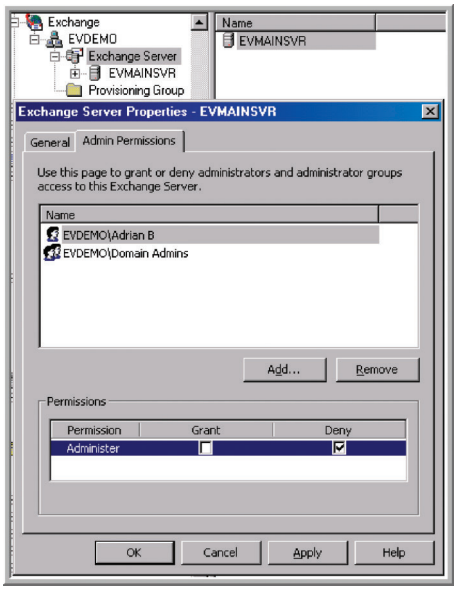


Figure 7. Assigning explicit restrictions to an Exchange Server.

For example, a Messaging Administrator who does not have access to a particular Exchange Server cannot enable mailboxes on that server, because the Enable Mailbox wizard does not allow the administrator to list the mailboxes on that server.

As soon as custom permissions are established on a particular object, access is immediately limited to that specific list of people, with all other administrators suddenly prevented from viewing the object, regardless of their role. To return to the state in which all administrators with the appropriate role have access to the container, all entries in the Administrator permissions list must be deleted. This can be helpful in situations where a specific geographic resource object (such as an Exchange Server or a file server) may be sensitive and need further restriction or access explicitly granted to an individual or small group.

Enterprise Vault operations monitoring and reporting

For those seeking insight into their archive system's health and trends, the Enterprise Vault operations monitoring and reporting module is a valuable resource. It monitors and reports on the status and health of applications in the archive.

Enterprise Vault Operations Manager

Enterprise Vault has historically allowed administrators to monitor the ongoing status and health of applications through standard Microsoft toolsets such as the Microsoft Management Console (MMC), Performance Monitor, and Microsoft Operations Manager. Often, however, administrators need to quickly and proactively track the health of various services over time, without requiring an MMC plug-in or the custom scripts and tools to do so.

Symantec offers just such capabilities through the Web-based Enterprise Vault Operations Manager (see Figure 8). The Enterprise Vault Operations Manager monitors local and remote Enterprise Vault servers, allowing administrators to:

- Review the status of Enterprise Vault services and tasks on any server in the same logical Enterprise Vault site.
- View Performance counters for vault stores, disk, memory, and processors.
- Monitor Exchange journal mailboxes using a number of message counters for Inbox, Archive Pending, and failed operations such as Failed Distribution List Expansion.

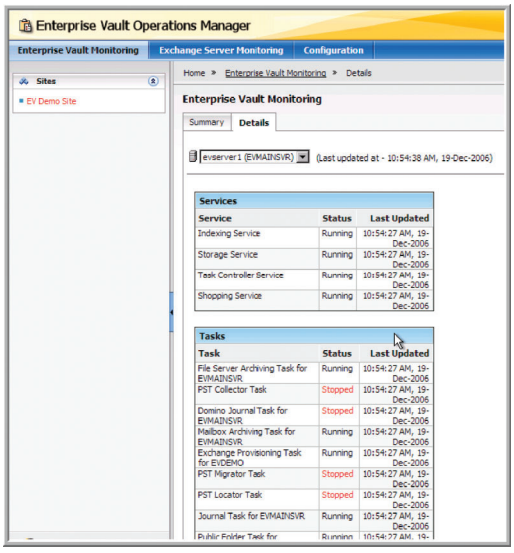


Figure 8. Enterprise Vault Operations Manager home page.

During an Enterprise Vault server installation, a monitoring agent can be automatically placed on each Enterprise Vault server. These monitoring agents collect data at scheduled intervals (every 15 minutes by default) and store it in the Enterprise Vault Monitoring database. The performance data will be stored in its own unique database, used exclusively by the operations monitoring and reporting modules.

In environments where archiving is necessary for compliance, legal, or discovery reasons, Enterprise Vault can archive a copy of all messages from a designated Exchange journal mailbox. In large environments, where journal mailboxes can grow quickly, monitoring of this mailbox becomes necessary to ensure that there are no backlogged messages or other failures occurring inside.

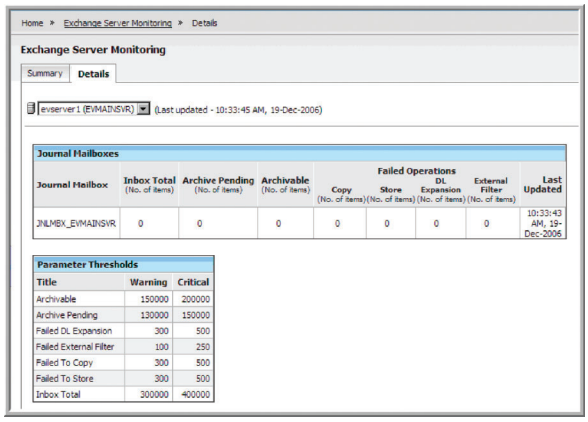
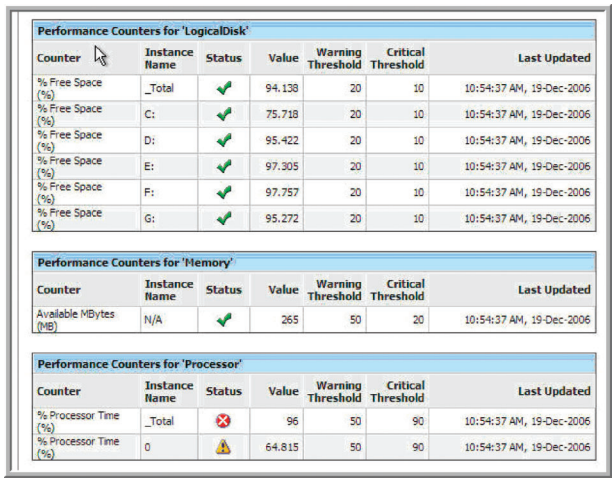


Figure 9. Journal Monitoring Report showing number of archived items and failures.

The Operations Manager gives administrators a view into the status of the journal mailboxes that are being archived, the numbers of messages archived from the journal, and a tally of errors for the monitoring period (see Figure 9).

From the Configuration page, administrators can enable or disable monitoring, adjust the frequency of the Monitoring agents polling the Monitoring database on the SQL Server, and modify the status indicator thresholds. These thresholds can be used to report on use cases with the Enterprise Vault Reporting module, described in the “Enterprise Vault Reporting” section. The module offers more detailed, historical reports about how Enterprise Vault has been running.

Based on the settings from the Configuration page, one can view a real-time status check of the Enterprise Vault Servers in the environment (Figure 10), scanning for warning or error icons where thresholds have been passed. These can flag an administrator to take action on a server or storage location where, for instance, a server is running low on free disk space or has low free memory available. By correcting these issues early on, an administrator can help prevent the archiving process from stopping or being disrupted.



Performance Counters for 'LogicalDisk'

Counter	Instance Name	Status	Value	Warning Threshold	Critical Threshold	Last Updated
% Free Space (%)	_Total	✓	94.138	20	10	10:54:37 AM, 19-Dec-2006
% Free Space (%)	C:	✓	75.718	20	10	10:54:37 AM, 19-Dec-2006
% Free Space (%)	D:	✓	95.422	20	10	10:54:37 AM, 19-Dec-2006
% Free Space (%)	E:	✓	97.305	20	10	10:54:37 AM, 19-Dec-2006
% Free Space (%)	F:	✓	97.757	20	10	10:54:37 AM, 19-Dec-2006
% Free Space (%)	G:	✓	95.272	20	10	10:54:37 AM, 19-Dec-2006

Performance Counters for 'Memory'

Counter	Instance Name	Status	Value	Warning Threshold	Critical Threshold	Last Updated
Available MBytes (MB)	N/A	✓	265	50	20	10:54:37 AM, 19-Dec-2006

Performance Counters for 'Processor'

Counter	Instance Name	Status	Value	Warning Threshold	Critical Threshold	Last Updated
% Processor Time (%)	_Total	✗	96	50	90	10:54:37 AM, 19-Dec-2006
% Processor Time (%)	0	⚠	64.815	50	90	10:54:37 AM, 19-Dec-2006

Figure 10. A server's Performance Counter settings.

Monitoring storage with the Event Viewer

In addition to the Enterprise Vault Operations Manager, Enterprise Vault offers the Event Viewer, which notifies administrators of potential issues with archiving, such as a backlog of items to be written to the archive or waiting to be backed up.

To enable this separate, built-in notification mechanism, an administrator simply configures the Site Properties in the Enterprise Vault Administration Console (see Figure 11). A set of alerts can be monitored, and parameters set to determine whether a warning is sent to the Event Viewer. For example, if Directory Backup has a threshold of two days, a warning is issued if the Enterprise Vault has not been backed up after two days. The application then rechecks on the next day, at the specified time.

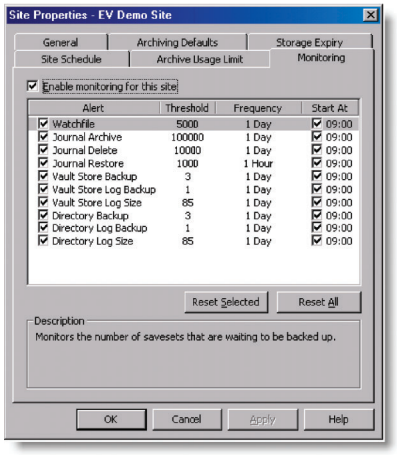


Figure 11. Event Viewer checklist of alerts that can be monitored.

Microsoft Operations Manager management pack

The Enterprise Vault is built upon a foundation of tight integration with Microsoft technology, and allows Symantec to easily leverage emerging Microsoft applications. This is exemplified by the optional preconfigured "management pack" offered for Microsoft Operations Manager (MOM). This Enterprise Vault management pack—provided on the Enterprise Vault server installation CD as a file called EnterpriseVault.akm—contains rules that enable the MOM to monitor critical Enterprise Vault events in the Application Event Log. MOM can also monitor and manage all the alerts on the Monitoring tab in Site Properties, as previously described. The MOM administrator enables/disables the preconfigured rules as needed, populates a computer group called Enterprise Vault (containing a list of all Enterprise Vault servers to be monitored), and populates a notification group called Enterprise Vault Administrators, so all appropriate administrators can be notified when an enabled rule is triggered.

Enterprise Vault Reporting

While Enterprise Vault Operations Manager is used to display the current health and activity on Enterprise Vault servers, Enterprise Vault Reporting offers a separate location for administrators to review and export historical trends occurring in the archive and with the servers. This Web-based application leverages Microsoft SQL Server Reporting Services (MSRS) as the mechanism for flexible report creation and display.

Enterprise Vault Reporting offers graphical answers to a manager's questions, and can provide responses to an administrator's curiosity about the health and growth of the archiving environment, using standard reports such as those listed in Table 1. Other reports are available, but these are the most likely to be accessed and used.

Table 1. Standard reports available with Enterprise Vault Reporting.

Report Name	Metric	Detailed Report information
Items Archived per Hour	How fast are we archiving?	This report shows, on an hourly basis, the total number of items archived, the total size of items archived, and the average size of items archived for a specific vault store or all vault stores collectively.
Mailbox Archiving Status	Is a particular mailbox enabled?	Displays whether a mailbox is enabled for archiving, and which policy is selected for it by the provisioning feature.
	How is a particular mailbox configured?	
Vault Usage Summary by Archive	How many items are in the archive?	Displays the size and status of each archive for the selected vault store.
Quota Usage Report	How close is an archive to its Enterprise Vault storage limit?	Displays the current size of archived items, and the archive usage limit for all archives.
Enterprise Vault Server Seven-Day Health Status	What percentage of time has my Enterprise Vault server been running? Has there been any downtime?	Displays the status of all Enterprise Vault services and long-running tasks on the Enterprise Vault server over the requested seven-day period. (**Note:** This module requires Enterprise Vault Monitoring to be enabled.)

Each report provides various parameters, such as time and server, in order to change the report's scope. Access to the reporting dashboard is available to any administrator who has been granted at least a Browser role via MSRS.

Figure 12. Enterprise Vault Operation Reports main page.

Clicking on any of the reports provides a view to the most current information relative to the parameters for that report (see Figure 12). The output can be formatted as an HTML, Excel, Web archive, PDF, TIFF, comma-delimited, or XML file (see Figure 13).

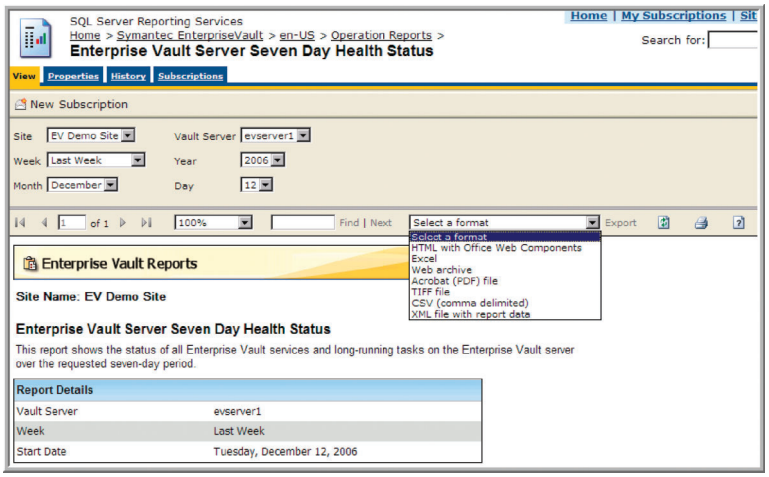


Figure 13. Reports offer options for date range and export format.

Report Delivery Options

Reports can be scheduled to run for export at specific intervals, with the target location being a file share or mailbox (see Figure 14). This can help in situations where evidence of service-level agreement compliance needs to be shown to external groups and users. For instance, an IT manager may want to know how much data is being archived each night; a storage administrator may need to know how close users are to their archive quota limits so their managers can be notified. Enterprise Vault can deliver the reports to a predictable location for a reliable review.

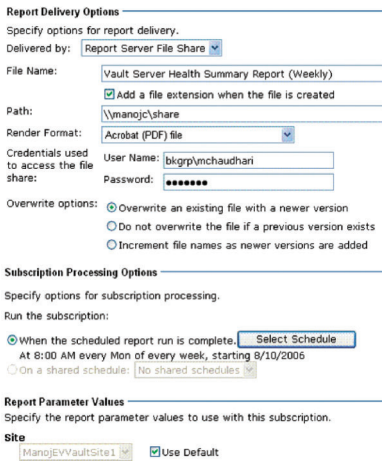


Figure 14. Options for report delivery.

Since SQL Reporting Services is a generic and flexible reporting application, administrators can build and store even more detailed and customized reports for future use. These custom reports can be stored on the main page, along with the standardized reports provided by default.

Symantec plans to build more standard reports, utilizing both the Monitoring capability as well as information stored within the Vault Store, Vault Directory, and optional Audit database.

Requirements for reporting

Requirements for Enterprise Vault Reporting:

- Microsoft Windows–based Server hosting IIS (Internet Information Services).
- SQL Server 2000 Reporting Services with SP2; or Microsoft SQL Server 2005 Reporting Services (SP1 recommended).

- Microsoft .NET Framework (for SQL 2005, Microsoft .NET Framework v2.0; for SQL 2000, version 1.1 or greater) stores collectively.

Enterprise Vault Reporting requires that you have already installed and configured the core Enterprise Vault components, as it communicates directly with the database server hosting the Enterprise Vault Directory database. You can install Enterprise Vault Reporting on a configured Enterprise Vault server if you have installed the prerequisites.

As the reporting leverages SQL Server Reporting Services, access to the reports is structured around its role-based authorization and Windows authentication, which determines who can perform operations and access items on the Report Server. The minimum and recommended level for accessing Enterprise Vault reports on the Report server is the Browser role.

Archiving simulation reports

In addition to the Web-based reports previously mentioned, Enterprise Vault offers built-in reports that allow administrators to test the impact of archiving on a defined range of users or mailboxes.

The *report mode* produces a test archive report on a selected task. In this mode, Enterprise Vault does not archive items, but produces a report showing what would be archived on a normal run. Figure 15 shows the screen for selection of archiving in normal or report mode.

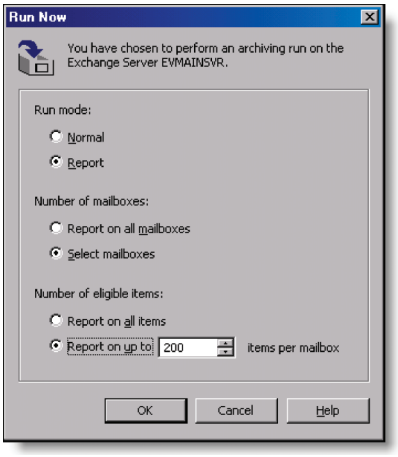


Figure 15. Creating a test report to verify what would be archived with a new Mailbox Archive policy.

The reports are logged in a text file in the Reports folder, a subfolder of the Enterprise Vault installation folder. The fields in the file are tab-separated, so you can easily import the file contents into a spreadsheet program such as Microsoft Excel®.

Other reports

Additional reports that can be generated by Enterprise Vault include the following:

- **Exchange mailbox preparation.** When processing provisioning groups, the Provisioning Task reports on mailboxes that have been prepared for archiving and the policies assigned.
- **Exchange mailbox archiving.** The report breaks down the current size of a user's mailbox, how large a user's mailbox will be after archiving.
- **PST migration.** In the case of Locate and Migrate there are separate reports for each phase of the migration: Location, Collection, and Migration.
- **Message export.** This can be used to review the export status of copying a portion of a mailbox archive to a PST file or to another user's mailbox.
- **File System archiving actions.** This report helps users review which files would be archived based on the policies and file servers selected.
- **SharePoint archiving actions.** These reports help users determine which sites and documents would be archived given the criteria selected.

Conclusion

When selecting an archiving platform, the enterprise must consider the organizational attention and expectations that will be placed on the IT infrastructure after implementation. The many challenges of enterprise-scale administration of archiving include:

- The need for many kinds of policies to satisfy a wide array of users at all different levels of the company
- How to leverage a distributed IT staff to administer the wide archive platform
- Monitoring and reporting on overall system health and trends occurring in the archive

As the leading archiving vendor, Symantec will continue its trend of innovation with the Enterprise Vault to meet and exceed ever-changing corporate standards for the management of electronic content.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Veritas, Enterprise Vault, and NetBackup are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft, Active Directory, Excel, SharePoint, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
2/07 11852912