WHITE PAPER: TECHNICAL

symantec™

Confidence in a connected world.

Security Model for Enterprise Vault 8.0 and SQL Server

Rob Forgione
Technical Field Enablement
February 2009

Contents

If you have any comments on this Whitepaper please email EV-TFE-Feedback@Symantec.com

Purpose

All of the whitepapers in this series will explain the following security aspects:

- How Enterprise Vault can securely access data to be archived
- How Enterprise Vault secures data in the archive
- The security surrounding end-user access
- How EV administrators can securely manage the solution

These whitepapers will detail how Enterprise Vault maintains data security and integrity through the use of Microsoft Windows Active Directory, components, and services as well as within various storage platforms. This document will give readers a better understanding of how the Enterprise Vault solution integrates with security features already built into Active Directory and provide insight as to how to change some of the settings to be configured in line with organizational preferences.

This whitepaper should be read first before reading the other Enterprise Vault Security Model whitepapers in the series. The Security Model series consists of:

- **Enterprise Vault 8.0 Security Model Enterprise Vault 8.0 and SQL server**
- Enterprise Vault 8.0 Security Model for Microsoft Exchange Archiving
- Enterprise Vault 8.0 Security Model for Lotus Domino Archiving
- Enterprise Vault 8.0 Security Model for File System Archiving
- Enterprise Vault 8.0 Security Model for Microsoft SharePoint Archiving
- Enterprise Vault 8.0 Security Model for SMTP Archiving
- Enterprise Vault 8.0 Security Model for Discovery Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Compliance Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Automatic Classification Engine 8.0
- Enterprise Vault 8.0 Security Model for Secure Messaging 8.0

This whitepaper is intended to train the reader the concepts behind Enterprise Vault 8.0 server and SQL server security.

Enterprise Vault Services and Tasks

The Enterprise Vault solution uses the following Core services that need to run no matter which archiving solution is being used. SharePoint, Domino, Exchange, SMTP and File System Archiving all use the same core services:

- Enterprise Vault Admin Service
- Enterprise Vault Directory Service
- Enterprise Vault Indexing Service
- Enterprise Vault Storage Service
- Enterprise Vault Shopping Service

Enterprise Vault also uses the following optional services that may not be present depending on the role of the server:

- Enterprise Vault Task Controller Service
- Enterprise Vault Accelerator Manager Service (for CA and DA)
- Enterprise Vault File Placeholder Service (for FSA)
- Enterprise Vault File Blocking Service (for FSA)
- Enterprise Vault File Collector Service (for FSA)
- Orchestria APM Infrastructure (for ACE Server role)
- Orchestria APM Policy Engine Hub (for ACE Hub role)
- Orchestria APM Policy Engine Server (for ACE Server role)
- Enterprise Vault Gateway Service for Secure Messaging and Rights Management

The Enterprise Vault Task Controller Service manages the following tasks:

- Domino Provisioning Task
- Domino Mailbox Archiving Task
- Domino Journaling Task
- Exchange Provisioning Task
- Exchange Mailbox Archiving Task
- Exchange Journaling Task
- Exchange Public Folder Task
- File System Archiving Task (for FSA and SMTP archiving)
- SharePoint Task
- PST Locator Task
- PST Collector Task
- PST Migrator Task

All Enterprise Vault Services are run under the context of the Vault Service account (VSA). Enterprise Vault Tasks are run under the context of the Vault Service account by default, but some can be changed to run using another account as necessary. If an account other than the Vault Service account is chosen, then it must have the appropriate permissions. The Vault Service account is discussed in greater detail in a later section.

Overview of the Enterprise Vault Solution

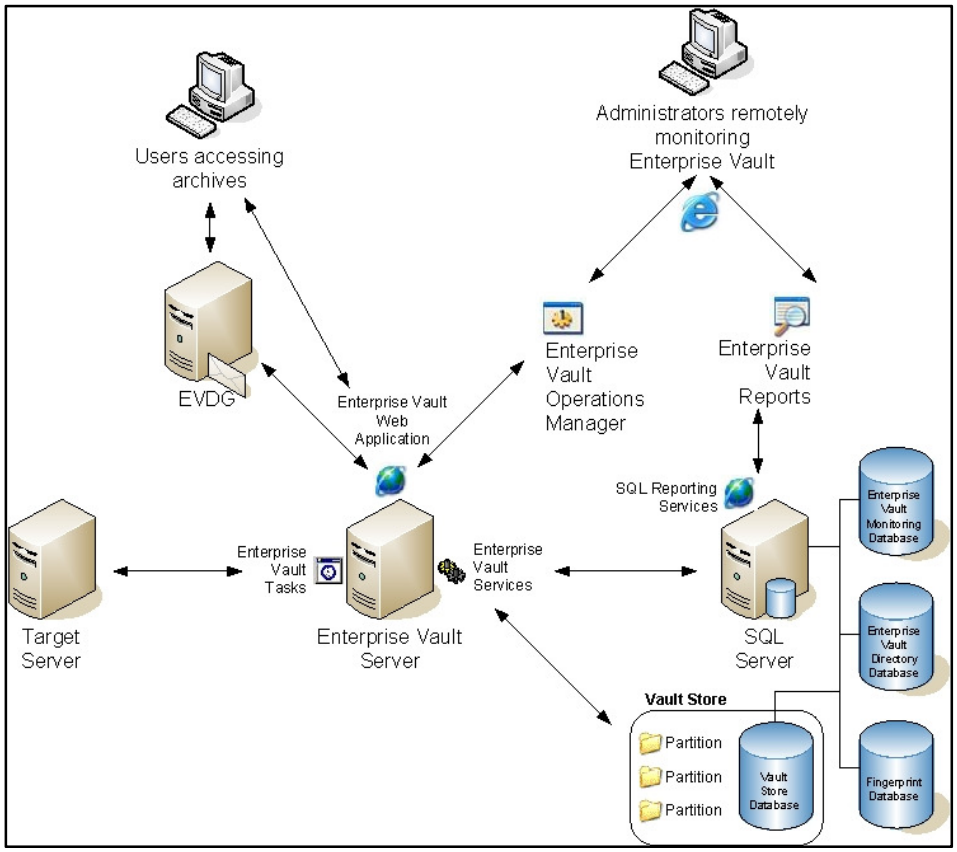
Enterprise Vault (EV) is a Windows application that enables an organization to store messaging and file system data automatically in centrally-held archives. Using Enterprise Vault clients, users can retrieve selected items easily and quickly when required.

Enterprise Vault **copies** items from source servers, referred to as Targets, and stores them in **archives**. They are then **indexed** to enable fast searching and retrieval. The solution, by default, will replace the original items with shortcuts that download and display the original item in its associated application. EV tools such as the browser search, Archive Explorer, Outlook/Lotus Notes User Extensions, and Outlook/Domino Web Access Extensions all provide:

- Access to archives
- Ability to search for archived items
- Management of archived items

Figure 1 gives a high level view of all of the components in a typical Enterprise Vault archiving solution. The "Target server" can be Exchange, SharePoint, Domino, and/or File Servers.

Figure 1 - Overview of archiving components



A common question that organizations ask is "How do I ensure maximum security of this solution without impeding normal operations?" Organizations must ensure the highest availability of data but avoid compromising it. This document will show how the Enterprise Vault security model secures these components, and the data contained within it, from day one of the installation.

Enterprise Vault Administration

The Vault Service account (VSA)

The Vault Service account is used by Enterprise Vault processes to access the Windows server operating system. The account is shared by all the Enterprise Vault servers in an Enterprise Vault Directory. The same VSA can be used to manage more than one Enterprise Vault Site.

The VSA must be an Active Directory domain-based Windows security account that belongs to the local Administrators group on all Enterprise Vault servers in the Enterprise Vault directory. This requirement is mandatory, even if an organization does not yet have an Active Directory (AD) infrastructure before implementation of the Enterprise Vault (for example, some Lotus Domino environments). This account should not be a member of the Domain Administrators group as Domain Administrators are often denied specific permissions that Enterprise Vault requires to perform archiving. It is better to assign required permissions explicitly. An existing administrator account used for another role within AD should never be used for the VSA. Because of the powerful nature of the VSA, using an existing AD administrator account could compromise an organization's security.

Whenever possible, the VSA should be in the same domain as the Enterprise Vault servers. If it is necessary for the VSA and the Enterprise Vault servers to be in different domains, the account must reside in a domain that is trusted by the Enterprise Vault servers' domain and ensure that the Microsoft Message Queue (MSMQ) security has been set up to grant the Administrators group access to the Enterprise Vault queues.

During the configuration of Enterprise Vault, the name and password of the VSA must be provided to the wizard. Once this is done, Enterprise Vault automatically grants VSA the following advanced user rights:

- Log On As a Service
- Act As Part Of The Operating System
- Debug programs
- Replace a process-level token

After creating the account, it may take some time for the VSA to be registered in the Active Directory for the server that is going to run Enterprise Vault. The account cannot be used until the registration is complete. Installers of the solution must be logged in as the VSA when installing and configuring Enterprise Vault.

Occasionally, there might be a need to change the VSA password. When changing the password, care must be taken to perform this in the correct location, otherwise the Enterprise Vault server will faill to function correctly due to incorrect DCOM security parameters.

Note that this is one of the reasons the VSA's password should be set to never expire when configured. Additionally, great care should be taken to ensure the VSA is not in an AD Group that inherits GPO's regarding automatic password expiry or change requirements.

Because it can be argued that administrative access to the VSA can be a security risk in itself, Enterprise Vault administrative access is further controlled by assigning roles and/or by using admin permissions. Many administrative tasks do not require all the permissions that are associated with the VSA. **Roles-based administration** enables organizations to provide individual Enterprise Vault administrators with exactly the permissions required to perform their individual administrative tasks only. Organizations can assign individuals or groups to roles that match their responsibilities. They are then able to perform the tasks that are included in those roles. As the permissions are associated with roles rather than individual administrators, roles can be edited without having to edit the permissions for each administrator. Additionally **Admin permissions** can be used to control access to containers in the Administration Console such as:

- Enterprise Vault Servers
- File Servers
- Exchange Servers
- Domino Servers
- SharePoint Virtual Servers

These administrative access methods will be explained in more detail below.

Roles-Based Administration

Out of the box, Enterprise Vault provides a number of predefined “administrator” roles. An administrator role is a collection of tasks, operations, and other roles:

- **Messaging Administrator:** Responsible for the day-to-day administration of Exchange Server and Lotus Domino archiving. This administrator does not have access to other parts of the product, such as File Server archiving or SharePoint archiving.
- **Domino Administrator:** Responsible for the day-to-day administration of Lotus Domino archiving. This administrator does not have access to other parts of the product, such as Exchange, File Server, or SharePoint archiving.
- **Exchange Administrator:** Responsible for the day-to-day administration of Exchange Server archiving. This administrator does not have access to other parts of the product such Domino, File Server, or SharePoint archiving.
- **File Server Administrator**: Responsible for the day-to-day administration of File System archiving. This administrator does not have access to other parts of the product, such as Exchange Server archiving or SharePoint archiving.
- **PST Administrator**: Has a view of the Administration Console that concentrates on the components required to manage the migration and disposition of PST (Microsoft Outlook personal store) files.
- **NSF Administrator**: Has a view of the Administration Console that concentrates on the components required to manage the migration and disposition of NSF (Lotus Notes personal store) files.
- **SharePoint Administrator**: Has a view of the Administration Console that concentrates on the components required to manage SharePoint archiving.
- **Storage Administrator**: Has a view of the Administration Console interface that concentrates on the components needed to keep the archive storage running properly. There is no access to archiving policy settings for the various targets.
- **Power Administrator**: Can perform all the tasks in the other predefined roles. Cannot perform reconfiguration tasks such as changing the VSA or Directory SQL server.

Organizations can use the predefined roles as supplied, customize them, or create new roles, as required. Only the Vault Service Account can alter or create new roles and assign permissions.

By assigning administrator roles, permissions of individual administrators can be adjusted to match their job responsibilities. The mechanism is flexible enough for organizations to be able to modify an individual's role to align with any subsequent change in responsibility.

Administrator roles can be assigned to the following:

- Windows Users and Groups
- The results of an LDAP query
- Application-specific groups

Application-specific groups are groups specific to Authorization Manager, that can contain a mixture of users and groups. Application-specific groups can also be based on a 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.

Best practice dictates that Windows Groups should be used to assist in managing Enterprise Vault through the use of Roles-Based administration. The concept is simple; apply Windows Groups to the EV Roles, then manage admin permissions to the VAC by moving users in and out of Windows Groups rather than editing the groups directly within the VAC. This eases Roles-Based administration by knowing that administrators have access to the VAC based on the AD Group they are members of. This is one example of how Enterprise Vault can leverage the organization's already existing Active Directory.

Figure 2 shows all of the available management containers within the Vault Administration Console (VAC). The administrative roles chosen for specific accounts will dictate what they can and cannot do within the console. In all cases, tasks that cannot be performed will be due to portions of the console that will not be viewable to the role.

Figure 2 - All available VAC options

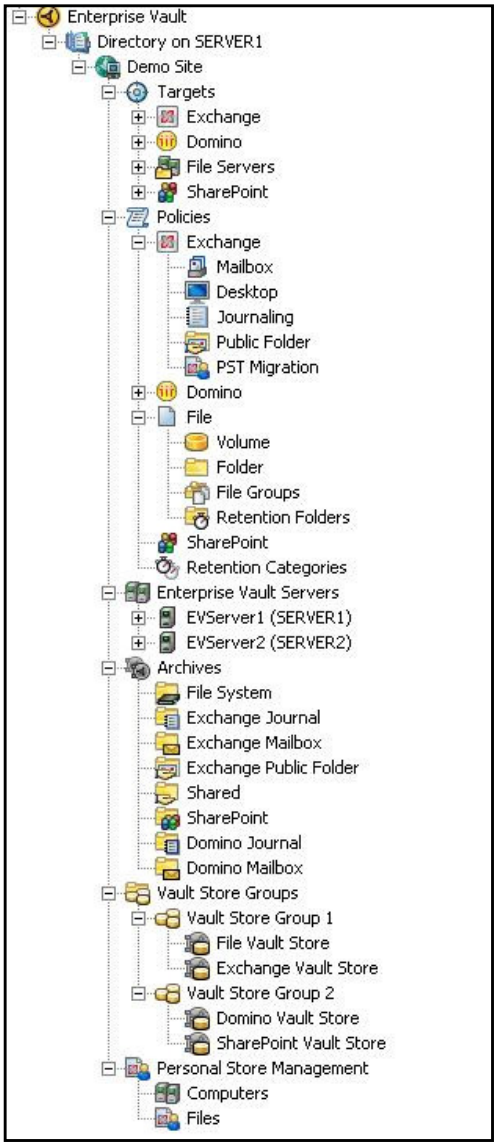
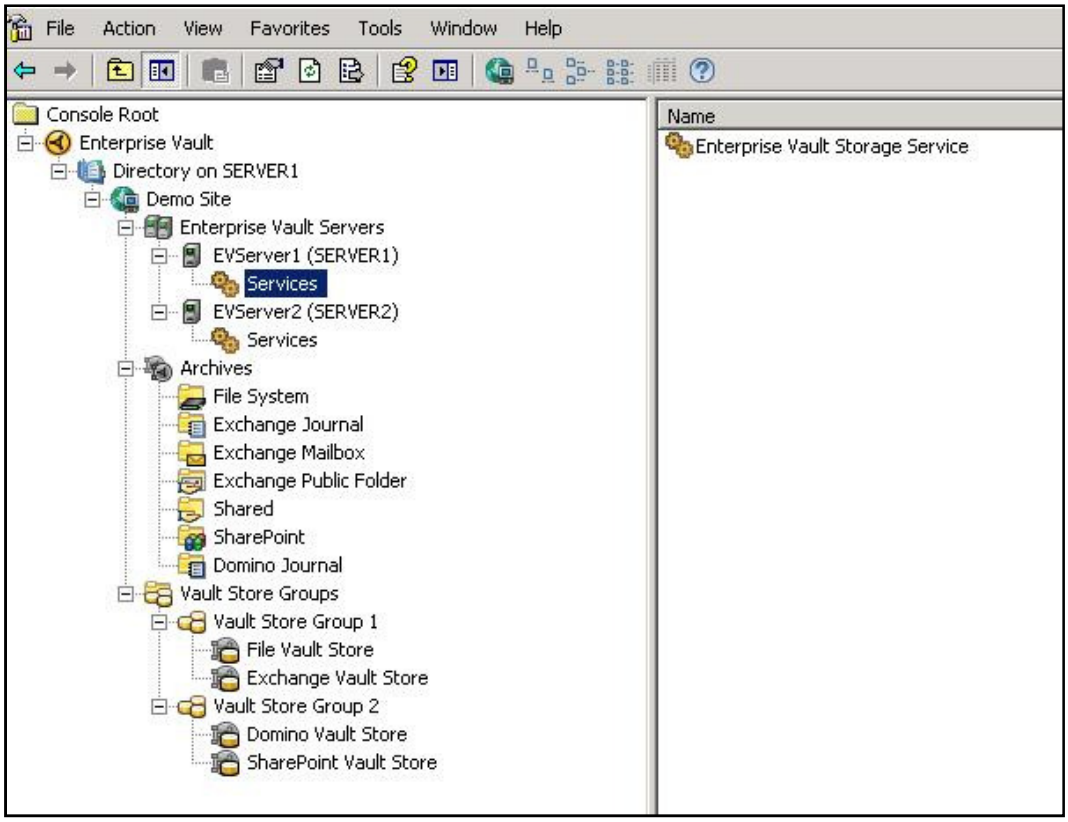


Figure 3 shows an example of the Storage Admin role. Note that the available containers and services are limited to the only functions a Storage Admin would require. Additionally, the ability to enable and disable mailboxes and workspaces are not available for this role, hence they have been grayed out from the toolbar.

Figure 3 - VAC display: Storage Admin role



Tables of the Administration Console containers and commands that are available for each role can be found in the Administrator's Guide PDF that ships with Enterprise Vault. Within the tables, it will be evident that a SharePoint Administrator for example, can enable SharePoint workspaces but not enable mailboxes for archiving. Messaging Administrator, which is a combination of Domino and Exchange roles, can neither import nor export archives. However, a PST Administrator, NSF Administrator, Storage Administrator, and Power Administrator can perform this function.

Admin Permissions

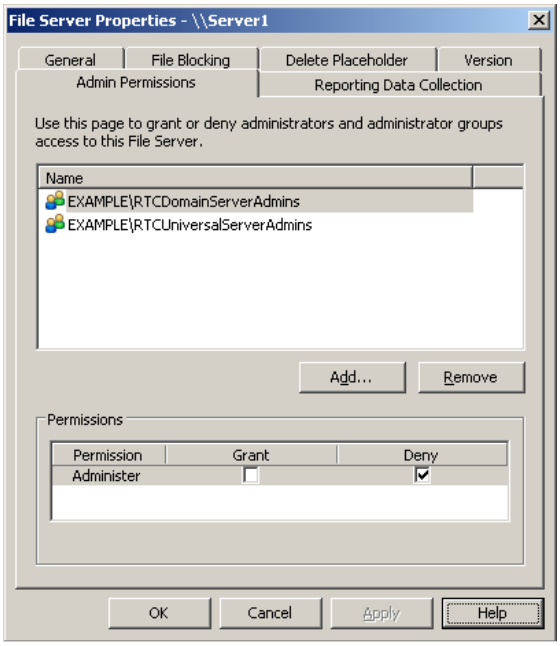
An administrator in any given role has access to all Administration Console containers that are relevant to that role. Administrator permissions can be assigned to grant or deny access to individual containers in the Administration Console, so organizations could grant one specific administrator account access to a single Exchange Server computer if necessary.

Permissions can be assigned to grant or deny access to any target including:

- Exchange Servers
- Domino Servers
- File Servers
- SharePoint Virtual Servers
- Enterprise Vault servers

Figure 4 illustrates a scenario in which DomainServerAdmins have been explicitly denied access to manage Server1. As soon as a container's permissions are modified, access to that container and its contents is controlled only by the administrators defined in the list. While the DomainServerAdmins cannot administer Server1, only members of UniversalServerAdmins can (explicit Grant permission not shown). The only exception to this behavior is that the VSA always has access. If it is necessary to return to the state in which all administrators have access to a container, all entries in the administrator permissions list must be deleted for that container.

Figure 4 - Admin Permissions for file server

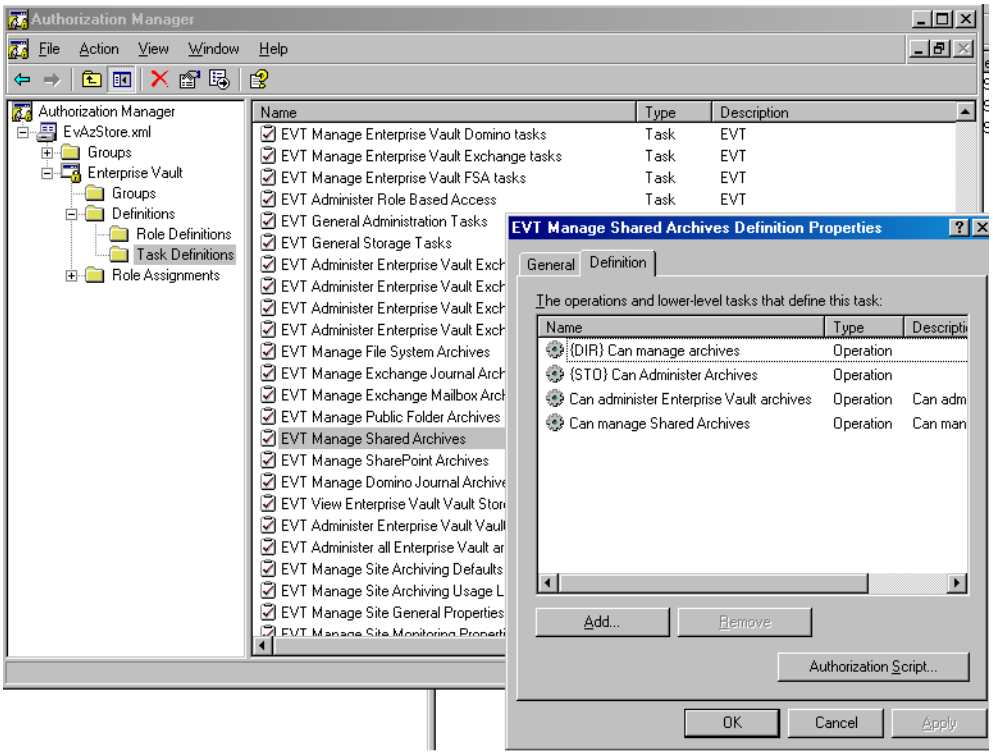


Custom Roles

It is possible through the use of Authorization Manager to customize predefined roles or create new roles as required. All such configuration is performed using the Vault Service account. The configuration of roles cannot be accomplished using Windows 2000 Server because Microsoft does not provide an Authorization Manager snap-in to run on Windows 2000 Server. Therefore, Windows 2003, XP, or later must be used.

Within Authorization Manager, administrator roles are built up using operations and tasks. Figure 5 shows the Authorization Manger interface.

Figure 5 - Authorization Manager



A **task** is a group of operations that collectively provide sufficient permissions to do a particular job. An **operation** is a low-level permission that represents a privileged action or capability. In the most basic sense, a **Role** is comprised of specific **Operations** grouped together as **Tasks**.

Important Note: Best practice dictates that organizations do not add individual operations to a role. It is recommended that tasks be used to create custom roles as tasks contain the correct combination of operations. Adding unnecessary operations to a role reduces the security of that role.

Remote Administration

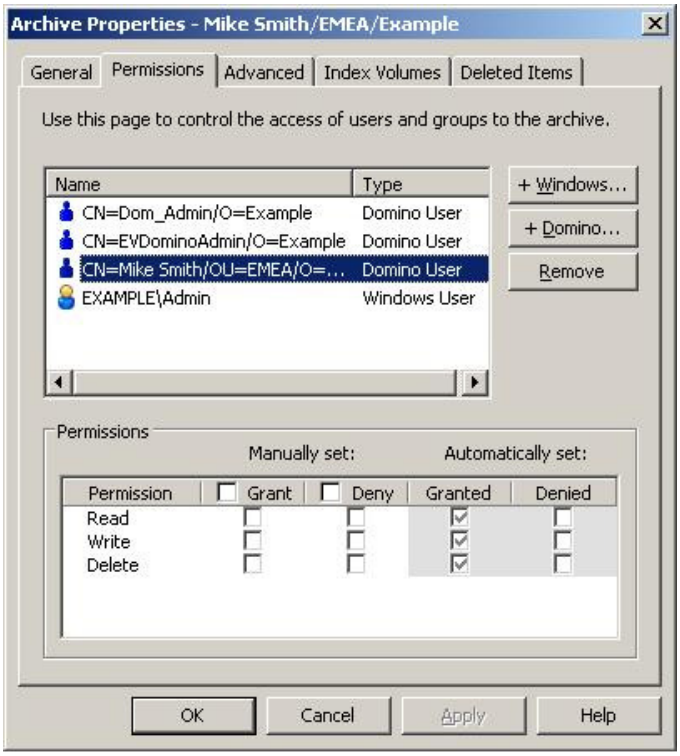
Using Roles Based Administration, administrators are assigned to roles and can administer EV remotely using the VAC from the MMC on their workstations. This removes the necessity of having to be logged into the remote workstation as the VSA in order to have permissions to manage properly.

Enterprise Vault administrators can also leverage the Enterprise Vault Operations Manager (EVOM) to monitor their environment. EVOM requires a Windows user account in order to access the Enterprise Vault databases on behalf of the administrative users. It is not recommended to use the VSA as this would defeat the purpose of using Roles. Therefore, it makes sense to create an account to be used only to monitor the environment.

Enterprise Vault Archive Security

Enterprise Vault leverages the Microsoft Active Directory security model for Exchange, SharePoint and File System Archiving. For Domino security, the Enterprise Vault Domino Gateway is used to integrate the Domino Security model into Active Directory. Simply put, if a user had access to the data before it was archived, they will have access after it is archived. More information about each specific security and permissions model is detailed in the respective security model whitepaper. Regardless of the type of target that is being archived, Figure 6 illustrates the universal security properties of an archive.

Figure 6 - User Archive Permissions



Within the dialog box, click any user in the list to display that user's permissions. The highlighted account in Figure 6 has inherited full access mainly because it is the mailbox owner.

The first set of two columns in Figure 6 shows permissions that are set manually. Check these to turn the permissions on or uncheck them to turn the permissions off.

The second set of two columns in Figure 6 shows the automatically granted and denied permissions. These are set when Enterprise Vault synchronizes the archive permissions to the source target permissions.

- **Read**: Accounts granted read permissions have access to all items in the archive. Those granted the Read permission can search, view, and restore items from this archive.
- **Write**: Accounts granted write permissions have the ability to store to the archive. Those granted the Write permission can store items in this archive.
- **Delete**: Accounts granted delete permissions are allowed to delete items from the archive. Those granted the Delete permission can delete items from this archive. But even if the delete permission is granted here, accounts cannot delete unless the "**Users can delete items from their archives**" checkbox is checked in the General tab of the Site Properties dialog box.

In some cases, permissions that are set either within Exchange folders or Enterprise Vault Policy Manager (EVPM) are managed behind the scenes in SQL and are not displayed in the Archive Properties dialog box. For example, an Executive Assistant only has permissions to Mike Smith's Calendar folder, therefore the Assistant is not shown in Figure 6.

Administrators can modify the manually set permissions as required. Manually set permissions always override automatically set permissions. For example, Deny Write permissions in the manual column override Granted Write in the automatic column. EVPM can be used to make bulk permission changes to multiple archives.

Enterprise Vault User Experience

Users of Enterprise Vault will notice subtle changes in the way they access information that has been archived. Content that has been archived will typically be replaced by shortcuts that trigger the download and display of archived content. Permissions for content within the archive are synchronized daily with the permissions configured in the content source, therefore only giving the authorized users access to the items just as they had prior to being archived. This model is consistent across Exchange, Domino, Sharepoint, and File System archiving, and is performed at an individual folder level (for example, an Accounting folder in the file system, a Calendar folder in one's mailbox, or a sensitive Public Folder).

Client Access Security

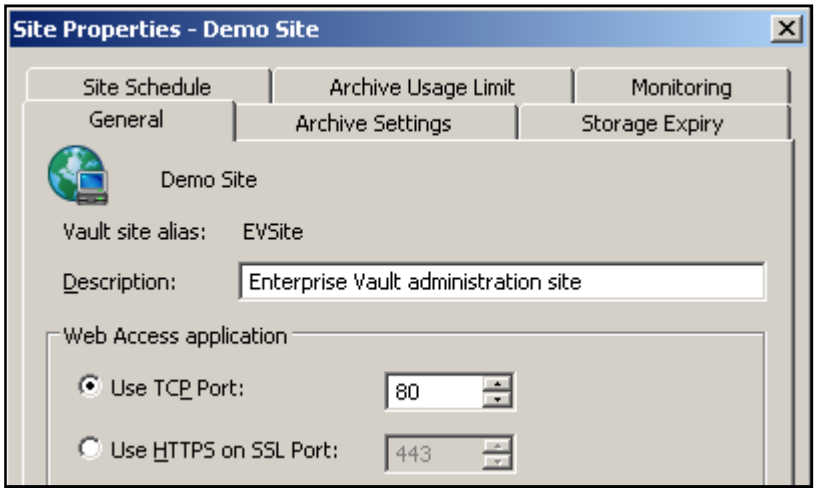
Enterprise Vault uses Microsoft Internet Information Services (IIS) and web-based security when any access to archived items is requested. For example, users double click on an Enterprise Vault shortcut which launches a command to retrieve the item. This action sends information about the requested item and the user making the request to a defined active server page in the EnterpriseVault virtual directory. The EV server verifies the requesting user by either Integrated Windows Authentication (IWA) or through a Basic authentication prompt.

After Enterprise Vault verifies the requestor, the EV server looks up the permissions of the item within the applicable vault store database and if it's deemed the user has access, the storage service will retrieve the item. The storage service (running as the VSA) calls the item from the storage device and sends the item to the client workstation, temporary mail database, or original file server depending on the archiving solution.

Enterprise Vault will not retrieve an item for a user it cannot authenticate. Therefore the *Enterprisevault* virtual directory for Exchange, SharePoint and File System archiving solutions, must never be set to enable anonymous authentication. The EnterpriseVaultDomino virtual directory however, does require this as it is the Enterprise Vault Domino Gateway instead of IIS that authenticates the requesting user. The applicable Enterprise Vault language subdirectories (**en** for example) should be set to enable anonymous access so the EV web pages render correctly.

It is also acceptable for organizations to use SSL to communicate from the client workstation to the Enterprise Vault server's virtual directory. This can be achieved by selecting the applicable port type and number in the General tab of the Site Properties. Figure 7 illustrates the options.

Figure 7 – Web Access application port options in the Site Properties



Vault Store Security

Enterprise Vault keeps all of the physical archived data in logical containers called Vault Stores. Vault stores are made up of one or more physical locations and one SQL database for metadata storage. The physical location is referred to as a Vault Store Partition. In any installation, the VSA is the only account that requires access to the storage location(s). Users do not require direct access to the partitions as all requests to view, archive, or delete data in that location are handled by the VSA on behalf of the user. When creating a Vault Store Partition, the option to **Create Vault Store Partition with security ACL's** is given. By leaving this option checked, Enterprise Vault will automatically grant VSA full permissions to the specified location. If the device chosen does not allow security ACL's to be granted remotely, simply uncheck the box and apply full permissions for the VSA manually per the device's documentation.

If the storage device is an EMC Centera, the Pool Entry Authentication (PEA) file provides Centera profile credentials that Enterprise Vault will use when connecting to the Centera. The PEA file must contain the minimum permissions for normal operation. These permissions are: Read, Write, Purge, Delete, Exist, and Query. If a PEA file is not specified, the Centera Anonymous account is used when connecting to Centera.

Index Location Security

Like the NTFS storage locations, the VSA is the only account that requires access to the index location(s). Users do not require direct access to the indexes as all search requests are handled by the Enterprise Vault Indexing Service using the VSA security context on behalf of the user.

SQL Server security

The Enterprise Vault environment typically involves 2 types of databases, though more can be expected depending on the features enabled: a Directory database that houses all of the solution's configuration information, and a Vault Store database that houses all of the information regarding the items stored within it. The VSA must be the database owner (dbo) of those databases. This requirement is easily satisfied during the prerequisite steps for installation. By giving the VSA a SQL login account with **Database Creators** permission for the SQL Server that will host the databases, the rest is taken care of by the EV server installation and/or configuration wizards. The Database Creators role allows the VSA to create the Directory database as well as any Vault Stores that are to be created. Once the EV databases are created, SQL automatically grants Database Owner (dbo) permissions to the VSA for the EV databases, and

the Database Creators role can be removed from the VSA. If minimal SQL permissions are required for the environment, then it is acceptable to grant the VSA DB_DATAREADER and DB_DATAWRITER permissions only, however these permissions will need to be elevated back to database owner if the solution is service packed or upgraded to a newer version.

If there is a future need to create another EV database (possibly due to a new vault store), simply place the VSA back in the Database Creators role, create the database, and then remove again if desired.

Ports used by Enterprise Vault

Table 1 shows the default Ports used by Enterprise Vault.

Table 1 - Enterprise Vault Ports

From	To	Source ports	Destination ports	Protocol	Comments
Clients	Domain Controller	Any	389	TCP	LDAP
Clients	Enterprise Vault	Any	80, (443), 135*	TCP	HTTP/HTTPS and DCOM (RPC)
Enterprise Vault	Domain Controller	Any	445	TCP	Microsoft DS
Enterprise Vault	Exchange Server	Any	135*	TCP	RPC (return port dynamically)
Enterprise Vault	NTFS File Server	Any	139, 445	TCP	CIFS and Microsoft DS
Enterprise Vault	SQL Server	Any	1433 (or other)	TCP	SQL
OWA Server	Enterprise Vault	80	455	TCP	HTTP/HTTPS
Enterprise Vault	SharePoint	Any	Defined by SharePoint	TCP	HTTP
Enterprise Vault	Domino Mail Server	Any	1352	TCP	NRPC

* = Dynamic return port

For an EV connection to an EMC Centera storage device through a firewall, port 3218 on the firewall must be open.

Compliance Accelerator and Discovery Accelerator both make the use of port 8085 which can be configured to use another port within their respective application config files. See the Enterprise Vault 8.0 Security Model for Compliance Accelerator 8.0 and Enterprise Vault 8.0 Security Model for Discovery Accelerator 8.0 whitepapers for more information.

Auditing

Enterprise Vault auditing records activity in a number of different categories (see Table 2). All auditing is disabled by default, but can be enabled, per Enterprise Vault server, to specify the categories that are to be audited. The output from auditing is written to the EnterpriseVaultAudit database that can be queried via Query Analyzer, EV Audit Viewer, or any other 3rd party reporting tool that can query data from SQL.

Table 2 - Auditable Events

This category	Records details of
View	Viewing archived items, either as HTML or in their original formats.
Delete	Archived items deleted manually. Enterprise Vault does not audit deletions that result from expiry.
Restore	Archived items being restored.
Archive	Items being archived, either manually or on a scheduled run.
PST Migration	Items being migrated from PST files.
NSF Migration	Items being migrated from NSF files.
Admin Activity	Configuration changes made in the Administration Console, such as adding a new service, creating archives, or enabling mailboxes.
Advanced Search	Searches performed using Outlook or the Web Access application, including the terms used and the number of items found.
Get Online XML	Document retrieval into SharePoint Portal Server.
SPS Archive	Items being archived from within SharePoint Portal Server.
User	Your own auditing entries, which you can add by calling a COM object that is served from the Admin Service. Supporting documentation provides VBS and ASP examples.
View Attachments	Viewing archived items from within SharePoint Portal Server.
FS Archive	Storage events from File System Archiving.
Domino Archive	Any Domino archiving activity
Domino Restore	Any Domino restore activity
Exchange Synchronization	Creation, modification, and deletion of Exchange managed content settings. Enterprise Vault records relevant details when it is configured to archive from Exchange managed folders and to synchronize with their managed content settings.
Archive Folder Updates	Saveset ID and source and destination folders of archived items being moved to a different mailbox folder.
Retention Category Updates	Changes to the retention category of archived items.

Enterprise Vault auditing does not log changes to role membership within Authorization Manager. For organizations that require auditing of changes within Authorization Manager, the use of the best practices described previously will satisfy this need. By assigning Enterprise Vault administrator roles to Windows security groups, Windows auditing can be used to track changes to those groups.

Conclusion

In this whitepaper we have discussed a large majority of the security aspects of Enterprise Vault 8.0. We have discussed how we keep information secure from unauthorized viewing and how we securely store archived data and indexes. We've also discussed administrative features like Roles Based administration, Auditing, and remote administration. Other relevant topics such as service accounts, Enterprise Vault communications security, and SQL data security were also discussed.

Now that you have a foundation in Enterprise Vault and SQL server security, you have the pre-requisite knowledge that will allow you to understand the security aspects around the other Security Model topics in this series:

- Enterprise Vault 8.0 Security Model for Microsoft Exchange Archiving
- Enterprise Vault 8.0 Security Model for Lotus Domino Archiving
- Enterprise Vault 8.0 Security Model for File System Archiving
- Enterprise Vault 8.0 Security Model for Microsoft Sharepoint Archiving
- Enterprise Vault 8.0 Security Model for SMTP Archiving
- Enterprise Vault 8.0 Security Model for Discovery Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Compliance Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Automatic Classification Engine 8.0
- Enterprise Vault 8.0 Security Model for Secure Messaging 8.0

About Symantec

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