WHITE PAPER: TECHNICAL

symantec.™

Confidence in a connected world.

Enterprise Vault 8.0 Security Model for File System Archiving

Rob Forgione
Technical Field Enablement
March 2009

Contents

Purpose 3

Enterprise Vault Services and Tasks 3

File System Archiving Security 4

Archiving from a Windows File Server 4

Archiving from a NetApp Filer 5

Archiving from an EMC Celerra 5

Access to items Archived from FSA 5

Access on Windows Platform 5

Access on NetApp Platform 6

Access on Celerra Platform 6

Conclusion 7

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

Purpose

The purpose of this document is to detail how Enterprise Vault:

- Can securely access data in file shares on file servers and other devices to be archived
- Provides secure access to archived files
- Provides administrators with a method of securing data

This document will give readers a better understanding of how the Enterprise Vault (EV) solution integrates with security features already built into Active Directory, NetApp Filers, and EMC Celerras. We will also provide insight as to how to change some of the settings to be configured in line with organizational preferences.

This whitepaper assumes the reader has already read the Security Model for Enterprise Vault 8.0 and SQL server whitepaper. The Security Model series consists of:

- 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 security for archiving data from file shares. It is also worth noting that this is the process used for SMTP archiving discussed in the Enterprise Vault 8.0 Security Model for SMTP Archiving whitepaper.

Enterprise Vault Services and Tasks

Enterprise Vault's File System Archiving solution uses the following Enterprise Vault Services and Tasks:

- Enterprise Vault Placeholder Service (found on file servers)
- Enterprise Vault File Blocking Service (found on file servers)
- Enterprise Vault File Collector Service (found on file servers)
- File System Archiving Task

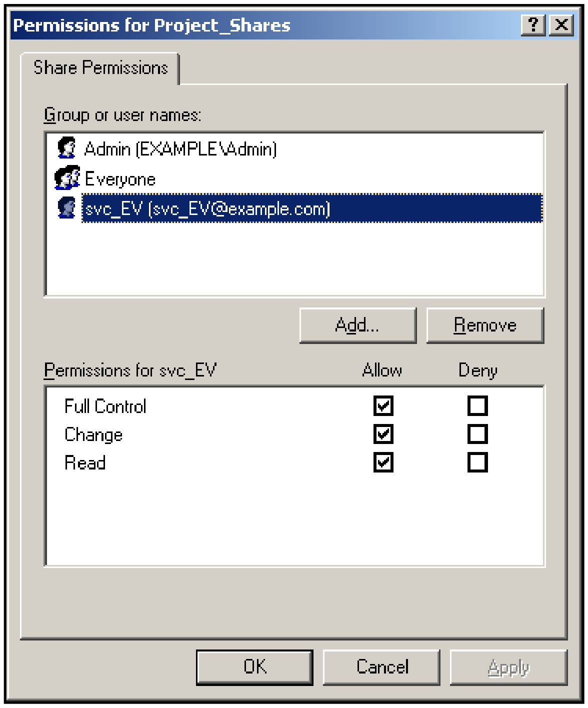
The Placeholder, File Blocking and File Collector services are referred to as the FSA Agent. The FSA Agent is not controlled by the Task Controller service running on the EV server.

File System Archiving Security

Archiving from a Windows File Server

On all file server targets, the Vault Service account (VSA) must be a local administrator and have Full Control of the share being used for the Volume target. Figure 1 shows an organization's VSA named svc_EV with the correct share permissions applied. This could be done through group membership as well.

Figure 1 - Share Permissions



Group or user names:

- Admin (EXAMPLE\Admin)
- Everyone
- svc_EV (svc_EV@example.com)

Permissions for svc_EV	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Browse permissions on volume target folders (or a folder in a folder path to a target) can be removed if corporate security enforces limitations administrators can have on "confidential" shares. If browse permissions do not exist, then the VSA will not be able to browse folders in the GUI during FSA configuration. EV can easily cope with this by requesting the administrator explicitly enter the path to the share when specifying the target folder.

When Enterprise Vault determines which users have access to an item archived within a folder, it looks to the permissions on the folder to synchronize with the archive. Enterprise Vault does not look to the permissions of the file itself due to synchronization performance issues. With this security model, it should be understood that an item with a set of permissions that do not match the folder permissions will inherit the **folder permissions** if the item is archived. To prevent this possible security issue, the option is available in the properties of the archiving policy to bypass archiving items that contain explicit permissions.

Archiving from a NetApp Filer

For organizations archiving from a NetApp Filer, the VSA must be added to the Administrators group on the NetApp file server. This gives EV the permissions needed to archive files and allow required fpolicy registration.

Archiving from an EMC Celerra

Organizations planning to use placeholder shortcuts on a Celerra must add the VSA to the Celerra administrators group. FileMover functionality on the Celerra must be enabled and an HTTP connection must be created. The most recent document containing these steps can be found here **http://support.veritas.com/docs/289676**.

Access to items Archived from FSA

Access on Windows Platform

Access to archived files can be accomplished in many different ways. One of the most common methods is the use of Placeholders. Another method is the use of Internet Shortcuts that act in a similar way to Placeholders. While Internet Shortcuts work well, they do not maintain the file type icon and thus do not maintain the seamlessness that many organizations desire. The third method of access is the use of Archive Explorer.

A placeholder shortcut is a sparse reparse point that appears exactly as the original file. When opened it forces Enterprise Vault to fetch the archived file. For placeholders to work, the VSA must have local administrator permissions on the target file server.

On NTFS file servers that host the Placeholder service, the Enterprise Vault server must be in the file server's Local Intranet Zone. This is typically achieved when the FSA Agent is installed. This requirement is due to Enterprise Vault making use of IIS and Web based security when it comes to users that are accessing archived items via placeholders or internet shortcuts. When a user double clicks on a Placeholder, the placeholder redirects the request to the Enterprise Vault virtual directory. The request sends the data specific to the item and requesting user information to the download.asp page on the EnterpriseVault virtual directory. The EV server then verifies the requesting user by either IWA or Basic authentication prompt as the Enterprise Vault virtual directory is configured by default to use Basic and Windows Integrated authentication (IWA).

If the Internet Explorer security settings are incorrect or not configured properly, users will not be able to open any placeholder shortcuts. Each attempt to do so will produce an "access denied" error in the Windows Application event log on the file server stating that there was an error downloading a file possibly because the requestor did not supply their account details. The event error is similar to the following:

```
Error downloading file: <file path>, <Saveset URL>
Error Account detail required, you must supply your account details [0xc004502d]
```

This commonly occurs because IWA is the only authentication method used to determine the requesting user. If any form of additional authentication needs to happen between requestor and EV Server, IWA will be stripped from the request. Enterprise Vault does not deliver items to entities it cannot validate and therefore results in this error. Ensuring the Enterprise Vault server in the target file server's Local Intranet Zone is the most common form of preventing this issue. Remember that the installation of the FSA Agent will attempt to perform this task automatically. If it can be verified that the agent was not able to do so, then this must be added manually while logged on the file server as the VSA.

After Enterprise Vault verifies the requestor, the EV server looks up the permissions of the item within the applicable store database. If it's deemed the user has access, the storage service calls the item from the storage device, sends it to the client requestor, and launches it in its native application.

Access on NetApp Platform

Access to items archived on a NetApp are accomplished via the Placeholder service that is run on the EV server. Placeholders on a NetApp are regular files with Alternate Data Streams containing the FSA Data.

Access on Celerra Platform

Access to items archived on a Celerra are accomplished via the Placeholder service that is run on the EV server. Placeholders on a Celerra are stubs created by the FileMover API.

Conclusion

In this whitepaper we have discussed the security aspects of archiving from NTFS file shares, NetApp Filers, and EMC Celerras with Enterprise Vault 8.0. We have discussed permissions required on the targets as well as the requirements necessary for end users to seamlessly access their archived files.

Below is a list of the other Security Model topics in this series that may be of interest.

- 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 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