WHITE PAPER: TECHNICAL

symantec™

Confidence in a connected world.

Enterprise Vault 8.0 Security Model for Automatic Classification Engine 8.0

Rob Forgione
Technical Field Enablement
February 2009

Contents

Purpose **3**

Enterprise Vault Services **4**

Automatic Classification Engine **4**

Account requirements 4

Conclusion **5**

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 the Intelligent Archiving components:

- Can securely access the Enterprise Vault archiving stream
- Provides a means for administrators to securely manage the applications

This document will give readers a better understanding of how the Enterprise Vault (EV) Intelligent Archiving solutions integrate with security features already built into Active Directory, SQL, and Enterprise Vault. It will also show how to manage access to the applications securely in line with organizational preferences.

This whitepaper assumes the reader has already read the Enterprise Vault 8.0 Security Model for Enterprise Vault 8.0 and SQL server whitepaper and is familiar with the security concepts of Enterprise Vault. 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 Microsoft Sharepoint 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 SMTP Archiving
- Enterprise Vault 8.0 Security Model for Discovery Accelerator 2007
- Enterprise Vault 8.0 Security Model for Compliance Accelerator 2007
- **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 the Automatic Classification Engine.

Enterprise Vault Services

Enterprise Vault uses the following Automatic Classification services.

- Orchestria APM Infrastructure (ACE)
- Orchestria APM Policy Engine Hub (ACE)
- Orchestria APM Policy Engine Server (ACE)

These services do not have a dependency on any other Enterprise Vault services.

Automatic Classification Engine

Enterprise Vault Automatic Classification Engine (ACE) enables Enterprise Vault to apply Smart Tagging rules when archiving messages from an Exchange Server mailbox. Smart Tagging is the intelligent categorization functionality in the Orchestria Active Policy Management (APM) solution. Specifically, it enables Enterprise Vault to apply rules to e-mails to categorize them according to their content or context.

Account requirements

On Base and Agent Machines

Vault Service account (VSA)

The VSA is required during the installation of ACE. It is used to set the VSA as the log on account used for the Orchestria APM Policy Engine Server service in Windows services. The VSA account is also used to generate a logon account for users to log into the ACE Policy Editor. This credential is stored in the engine's central management database and is **not reflective of the VSA afterwards**. In other words, if the VSA changes later, this will not be reflected in ACE. In keeping with the Roles-Based security model discussed in Enterprise Vault 8.0 Security Model Enterprise Vault 8.0 and SQL server, the password used to log into the ACE Policy Editor should be changed immediately after installation to prevent possible misuse (this will NOT affect the VSA password for the EV solution). The VSA must be a member of the Administrators group on the ACE Base servers.

On Base Machines Only

Database administrator

The ACE Database Administrator account must have full administrator rights for the SQL Server database on the Base machine. The installation wizard uses this account to create a new SQL Server login that ACE will use to access the central management database.

Conclusion

In this whitepaper we have discussed the security aspects of the ACE database and Policy Editor web access.

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 Discovery Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Compliance Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Secure Messaging 8.0
- Enterprise Vault 8.0 Security Model for File System Archiving
- Enterprise Vault 8.0 Security Model for SMTP Archiving
- Enterprise Vault 8.0 Security Model for Microsoft Sharepoint Archiving

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