Backup Exec 12.5 and Enterprise Vault 8.0

Protecting EV 8 with Backup Exec 12.5's Agent for Enterprise Vault

Confidence in a connected world. symantec.

BACKUP EXEC 12.5 AGENT FOR ENTERPRISE VAULT and ENTERPRISE VAULT 8.0

Key Takeaways

- Supports Enterprise Vault 7.5 and 8.0
- Combination of manual jobs and Agent for Enterprise Vault jobs offer complete protection for Enterprise Vault
- Customers who use the Agent for Enterprise Vault do not need to purchase additional agents

Backup Exec 12.5 released an Agent for Enterprise Vault, which is designed to offer complete protection for Enterprise Vault 7.5 implementations. When Enterprise Vault 8.0 was released, architectural changes in EV 8.0 made the Backup Exec 12.5 Agent for Enterprise Vault unable to automatically protect all aspects of Enterprise Vault.

This White Paper describes how to use the Backup Exec 12.5 Agent for Enterprise Vault with Enterprise Vault 8.0 to provide complete protection for EV 8 databases, Vault Stores, Indexes, and Partitions.

For customers who have not purchased the Agent for Enterprise Vault, and wish to protect Enterprise Vault manually with a combination of Backup Exec Agent for SQL Server and Agent for Windows Systems, refer to the following Tech Note:
http://seer.entsupport.symantec.com/docs/312327.htm

The Backup Exec 12.5 Agent for Enterprise Vault contains all of the building blocks necessary to protect Enterprise Vault 8.0. Customers who have purchased the Agent for Enterprise Vault do not need to purchase any additional Agents/Options to fully protect Enterprise Vault with Backup Exec.

Platform Support

- Enterprise Vault: Enterprise Vault 8.0
- Hardware and OS: Windows 2000 (x86-32bit), Windows Server 2003 (x86-32bit and x64-64bit) Windows Server 2008 (x86 and x64)
- Clustering: Enterprise Vault Cluster on Microsoft Cluster Services (MSCS)
- Databases: SQL 2000 (SP3 and later), SQL 2005 (SP2 and later).
- NAS devices: Backup NAS devices using CIFS
- NetApp/EMC: NDMP devices (as partitions)

Background

The Backup Exec 12.5 Agent for Enterprise Vault provides consistent backup and recovery services for Enterprise Vault installations. The Agent integrates with Enterprise Vault to do the following:

- Display the Enterprise Vault Infrastructure in a simple and logical manner in the Backup Exec Administration console
- Enables and disables Enterprise Vault's backup mode, so databases, Vault Stores, Indexes, and Partitions are able to be backed up consistently
- Allows recovery of individual indexes, files in partitions, partitions, Vault Stores, and databases.

Enterprise Vault 8.0 has added several additional databases as part of its default installation. These databases are the Audit, FSA Reporting, and Fingerprint databases. These additional databases are not automatically protected by the Agent for Enterprise Vault and must be protected manually. The process below will outline how to create the necessary jobs to fully protect Enterprise Vault 8.0 with the Backup Exec 12.5 Agent for Enterprise Vault.

BACKING UP ENTERPRISE VAULT 8.0

The following procedure will create several jobs which will result in complete protection for the Enterprise Vault 8.0 infrastructure.

Step 1

When the Agent for Enterprise Vault is installed on each member server in the Enterprise Vault infrastructure, the Enterprise Vault entities shown in the Backup Browse view will form the core of the first job. From the Backup View, expand the "Enterprise Vault" icon, and select the Sites,

Vault Stores, Vault Store Databases, Partitions, Index Locations, Directory Databases, and Monitoring Databases to be backed up in this first job.

This will create a single job that protects these specific entities. This job will keep the EV Services in read-only mode for database consistency purposes.

Step 2

Create a series of SQL jobs to protect the additional databases introduced in EV 8.0. These databases are the Auditing Database (AuditDB), the FSA Reporting Database (FSAReportingDB), Fingerprint Database (FingerPrintDB), Compliance Accelerator, and Discovery Accelerator databases.

Administrators will need to browse to the appropriate physical server where these databases run in order to select them for protection. The Agent for Enterprise Vault must be licensed and the Remote Agent for Windows Systems must to be installed on any system that hosts an Enterprise Vault database.

These databases do not require Enterprise Vault to be put into ReadOnly or backup mode, and as such can be protected while they are online. The Agent for Enterprise Vault includes all features and functions necessary to consistently protect running Microsoft SQL databases.

1. Create a SQL backup job to protect the Auditing Database (EnterpriseVaultAudit) and the FSA Reporting Database (EnterpriseVaultFSAReporting)
    a. Use Full or Incremental (backup transaction log and truncate) backup method.
2. Create a SQL backup job to protect the Fingerprint Database and ExpressVaultStore Databases
    a. Use Full, Differential, or incremental (backup transaction log and truncate) backup method.
    b. Symantec advises customers to backup the FingerPrint databases after every VaultStore backup. This is to ensure that backup copies of the Fingerprint Database and the physical VaultStore are consistent. In case of a recovery, the closer the FingerPrint Databases and VaultStores are in time will make for a faster recovery process.
3. Create a SQL backup job to backup Compliance Accelerator and Discovery Accelerator databases (i.e. ConfigurationDB, CustomerDB and CustodianDB) if present.
    a. Protect Configuration, Customer, Custodian, and other databases using Full, Differential, or Incremental (backup transaction log and truncate) backup methods.

Note in **Figure 1** below, there are number of Enterprise Vault databases on the selected server **sql.almond.local**. In the right pane, there are a mix of greyed-out (not selectable) and selectable databases. The databases to be selected for protection in this second job are outlined in red.
The grayed-out databases are those automatically protected by the first job, configured in step 1.

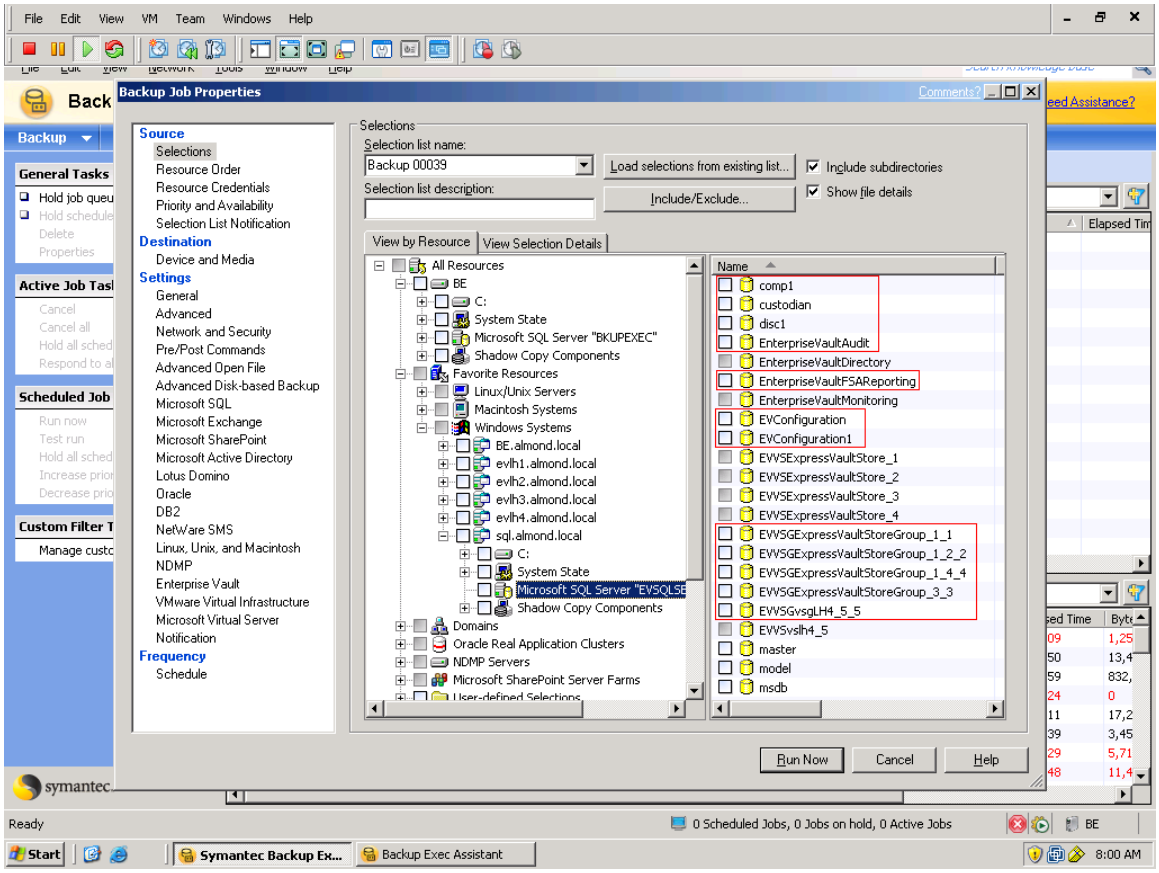

Figure 1 *– Enterprise Vault databases to be protected in step 2.*

Notes regarding Enterprise Vault Database names

This document

- Fingerprint Databases and Vault Store Group database names start with EVVSG.
- FSAReporting DB and Auditing DB can be identified by their names itself. In above image you can see EnterprisevaultAudit and EnterpriseVaultFSAReporting are the respective DBs for Audit and FSA reporting
- While doing initial installation and configuration for the Compliance Accelerator and Discovery Accelerator, customers can specify the database names for these components. Thus, a customer's configuration may have different database names than are represented in figure 1. In the example in Figure 1, the Compliance and Discovery Accelerator databases are named "EVconfiguration" and "EVconfiguration1" respectively.

RESTORING ENTERPRISE VAULT COMPONENTS

There are several methods for recovery of servers or Enterprise Vault components/entities depending on the severity of recovery needs.

Restoring the entire Enterprise Vault infrastructure

If an entire machine needs to be rebuilt, the OS, Enterprise Vault, Compliance Accelerator, Discovery Accelerator, and RAWS will need to be reinstalled before restores can take place. As is usual with full machine recovery, full backups and then any incremental/differential backups should be restored.

Listed here is a sample outline of a complete recovery process. Use the following steps as a guideline to create an applicable recovery process.

1. Run a restore job for the Directory and Monitoring databases
    a. Use the "Terminate connection…" option found in the Restore Job Properties -> Enterprise Vault section for this recovery
2. Run a restore job for VaultStore databases, Partitions (both open and closed), and Index locations
3. Manually stop the Enterprise Vault services while restoring the FingerPrint database, Auditing Database and the FSA Reporting Database. If you don't want to stop the services then you need to make database offline from SQL restore page.
4. Run a restore job for the FingerPrint database
5. Run a restore job Auditing Database and the FSA Reporting Database
6. Run a restore job for Compliance Accelerator and Discovery Accelerator databases
    a. Symantec recommends Administrators take these databases offline or stopping the Enterprise Vault Accelerator Manager Service prior to recovery.

Restoring one or more Enterprise Vault entities

If one or more Enterprise Vault entities need to be recovered, the recovery method depends on the recovered resource. The following sections cover restoring individual entities from backup copies generated by backup jobs created in the section "Backing Up Enterprise Vault" above. Administrators should also read the Backup Exec Administrator's Guide for details about the Agent for Enterprise Vault.

1) Recovering Fingerprint DB, Audit and FSA Reporting Databases

Stop the Enterprise Vault services manually and recover the Auditing or FSA Reporting Databases as you would any other SQL database. If you don't want to stop the Enterprise Vault services, then take the databases offline before performing any recoveries.

Restore Full backups, then any incremental/differential backups

2) Recovering Compliance Accelerator and Discovery Accelerator databases

Stop the Enterprise Vault Accelerator Manager Service or take the databases offline before performing any recoveries.

Restore Full backups, then any incremental/differential backups

3) Recovering VaultStore Databases, Partitions, Indexes, and Directory and Monitoring Databases

Use the functionality provided by the Agent for Enterprise Vault to recover these entities. Refer to the Backup Exec 12.5 Administrator's Guide for additional details on recovering these entities. See Figure 2 for an example of the Enterprise Vault entities recoverable via the Agent for Enterprise Vault.

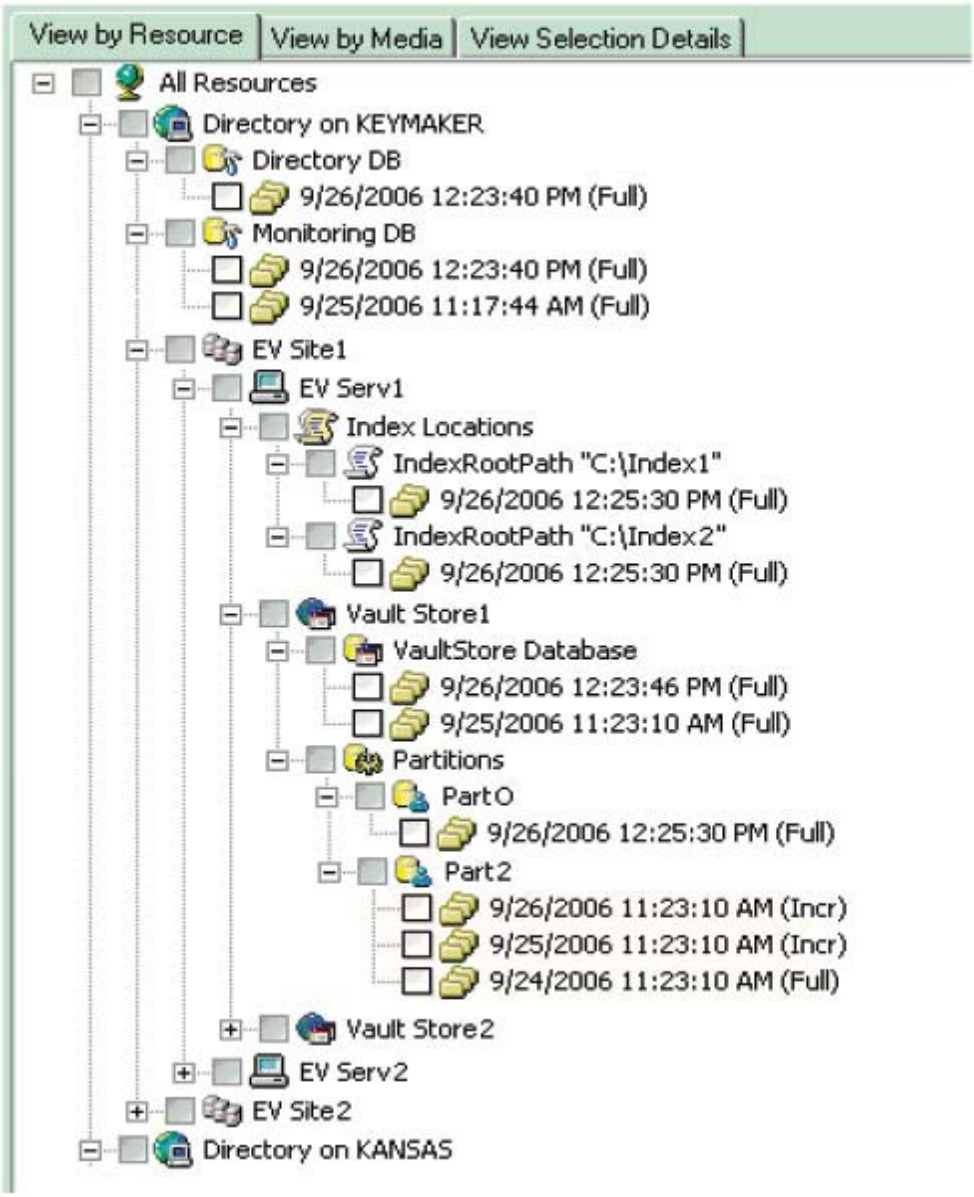

Figure 2: *Using Agent for Enterprise Vault features to recover some of the Enterprise Vault Entities*

NOTES FOR RESTORE JOBS

1. If the restore is a Full backup followed by an incremental or differential chain:
    a. For recovery of a Full backup of entities protected by the Agent for Enterprise Vault: Select "Leave Database non-operational…" option in the Enterprise Vault recovery options while restoring the full backup.
    b. For recovery of Incremental or Differential backups: select the "Leave database ready to use…" option in the Enterprise Vault recovery options while restoring incremental or differential backups.
2. Use "Restore Over Existing…" from the SQL Server recovery options while restoring the any of the SQL Databases not protected by the Agent for Enterprise Vault

Appendix A: Clustering Support with the Backup Exec 12.5 Agent for Enterprise Vault and Enterprise Vault 8.0

Because of the changes in Enterprise Vault 8.0, Backup Exec does not automatically support backup and recovery of Enterprise Vault running in a cluster. To correct this, administrators will need to add a registry key to all nodes in the cluster.

In the following example, the name "EV1" is the name of cluster virtual node and resource group.

Add following registry key (**string** value type)

Windows 32-bit

[HKEY_LOCAL_MACHINE\SOFTWARE\KVS\Enterprise Vault\Admin\ConfigState]
"ClusVirtualServer"="EV1"
"ClusResourceGroup"="EV1"

Windows 64-bit

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\ENTERPRISEVault\Admin\ConfigState
"ClusVirtualServer"="EV1"
"ClusResourceGroup"="EV1"

Administrators should note that the Agent for Enterprise Vault does not support VCS clusters.

BACKUP EXEC AGENT FOR ENTERPRISE VAULT LICENSING

Backup Exec Agent for Enterprise Vault is licensed per Enterprise Vault server. Backup Exec 12.5 for Windows Servers is designed to accommodate the needs of Windows-based environments of all sizes– whether it's a single Windows Server or a large, multi-Domain Windows enterprise including multiple remote Linux and UNIX servers. The Backup Exec 12.5 Windows Server portfolio provides a wide array of high powered Agents and Options which are licensed on a per-Server or per-storage device for added scalability, supporting all Windows 2000, 2003 and 2008 environments, physical or virtual servers, and unlimited processors on the system

Scenarios	Customer Environment	Licensing
Protecting a Single-Server Enterprise Vault configuration	1 Media Server 1 Enterprise Vault Server Directory, Monitoring, and Vault Store databases, and local partitions	Qty:1 of Backup Exec 12.5 for Windows Server license Qty:1 of Backup Exec 12.5 Agent for Enterprise Vault
Protecting multiple Vault Stores on different Windows computers	1 Media Server 1 Enterprise Vault Server with Directory, Monitoring, and Vault Store Databases Five Windows Servers with Vault Store partitions and index locations	Qty:1 of Backup Exec 12.5 for Windows Server license Qty:6 of Backup Exec 12.5 Agent for Enterprise Vault

Backup Exec 12.5 and Enterprise Vault 8.0

Protecting EV 8 with Backup Exec 12.5's Agent for Enterprise Vault

Confidence in a connected world. symantec.

INTEGRATED DATA PROTECTION

Symantec Backup Exec 12.5 for Windows Servers can be expanded to protect additional remote systems and applications through the purchase additional Agents and Options which enable administrators to design and easily implement a comprehensive data and system protection solution for any Windows server environment. Other Backup Exec 12.5 agents & options that compliment the Backup Exec Enterprise Vault include:

• **Agent for Windows Servers**	• **Advanced Disk-based Backup Option**	• **Central Admin Server Option**
• **Agent for Exchange Servers**	• **SAN Shared Storage Option**	• **Agent for Lotus Notes Servers**

FOR MORE INFORMATION

Symantec Enterprise Sales Support: 800-745-6054
Backup Exec on the Symantec Web Site : http://www.backupexec.com