Enterprise Vault Whitepaper

Enterprise Vault Integration with Veritas Products

This document provides an overview of the integration points between Veritas Enterprise Vault and other Veritas products

This document applies to the following version(s) of:

- Enterprise Vault 9 and later
- Enterprise Vault.cloud
- eDP 7.0 and later
- Data Insight 4.0 and later
- Veritas Information Map
- NetBackup 7.5 and later
- Veritas Storage Foundation/InfoScale 6.0 and later

If you have any feedback or questions about this document please email them to II-tec@veritas.com stating the document title.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Document Control

Contributors

Who	Contribution
Evan Barrett	Author
Liam Finn	Contributor
Chris Ebner	Contributor

Revision History

Version	Date	Changes
1.0		Initial release

Related Documents/Links

Document Title	Version / Date
Veritas Technical Partner Program http://go.veritas.com/vtpp	N/A
Integrating eDiscovery Platform 8.2 and Enterprise Vault 12.0.1 https://www.veritas.com/support/en_US/article.000125192	December 2016
Backing up Enterprise Vault https://www.veritas.com/support/en_US/article.000010873	October 2015
Migrating Enterprise Vault Content to NetBackup http://www.veritas.com/docs/000070836	December 2016
Data Insight 5.2 Feature Briefing – Metadata Framework http://www.veritas.com/docs/000125198	December 2016

Table of Contents

Introduction

Those who work with Enterprise Vault often inquire about how it integrates other Veritas products. Although this whitepaper will not spell out best practices, it does provide details of the integration points between these products.

The first few sections of this document will detail the integration points with Enterprise Vault and Information Intelligence products. These products include Enterprise Vault, Enterprise Vault.cloud, Data Insight, and eDiscovery Platform.

The remaining sections of this document will detail integration of Enterprise Vault with other Veritas products such as NetBackup and Storage Foundation/InfoScale.

Enterprise Vault and Data Insight

Currently, the integration between Enterprise Vault and Data Insight consists of the ability of Data Insight to initiate the archiving of identified files to Enterprise Vault. The archiving process can be initiated through an action as of a result a report generated in Data Insight or through the use of the Data Insight Workspace. Integration is supported with Enterprise Vault 10.0.4 or later and Data Insight 4.0 and later.

There are many use cases for the integration between Enterprise Vault and Data Insight:

- Quickly identify data that is orphaned (as identified by Data Insight) and archive it with Enterprise Vault – As users leave an organization, they may have old files that may have been left behind. Data Insight can identify these files and instruct Enterprise Vault to archive them freeing up disk space on the file server/filer.
- Archive data that has been identified as sensitive and delete from the file server – Files may contain sensitive data such as credit card numbers or other personal information. These identified files can then be archived by Enterprise Vault and removed from the file server/filer. Archived content can then be further examined through compliance and eDiscovery processes.
- Archive select folders within a file share – An organization may not wish to fully archive all folders on a file share and only archive certain files or folders (such as a completed projects). Data Insight can initiate the archiving process of these selected files and folders to Enterprise Vault.
- Starting with Data Insight 5.2, the Metadata Framework feature can assist with the classification of file system data by tagging files, folders, and shares with attributes. This classification process can then be used during reporting to identify files that meet desired criteria that should then be archived by Enterprise Vault.

Before archiving can take place, it is necessary to create a saved credential for the Enterprise Vault Service Account (VSA) and configure Data Insight to communicate with Enterprise Vault by adding the server as a Data Management device within Data Insight. This is necessary to discover Enterprise Vault Retention Categories and archiving policies. It will also be necessary to configure the file share as an archiving target in Enterprise Vault. Once the file has been archived, it can be either deleted, replaced with a placeholder/shortcut, or left alone. The integration process is highlighted in Figure 1.

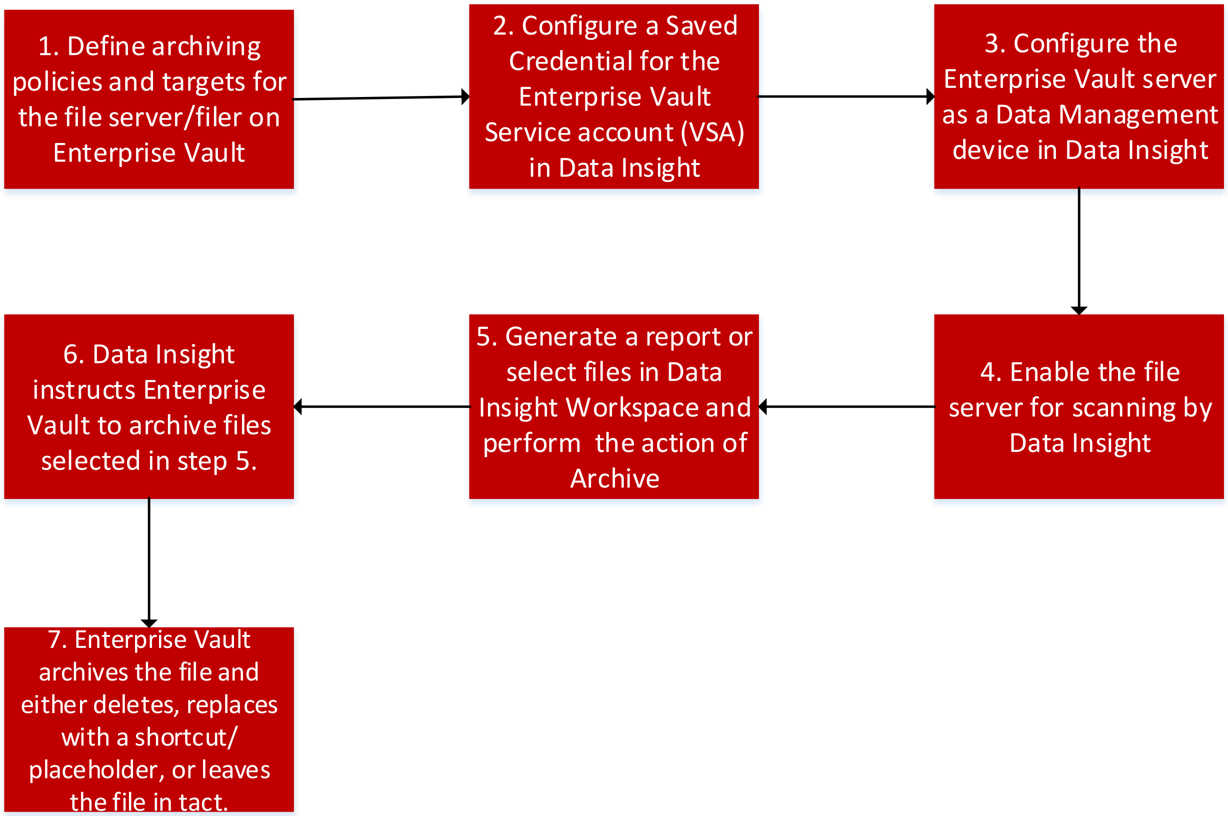
1. Define archiving policies and targets for the file server/filer on Enterprise Vault
2. Configure a Saved Credential for the Enterprise Vault Service account (VSA) in Data Insight
3. Configure the Enterprise Vault server as a Data Management device in Data Insight
4. Enable the file server for scanning by Data Insight
5. Generate a report or select files in Data Insight Workspace and perform the action of Archive
6. Data Insight instructs Enterprise Vault to archive files selected in step 5.
7. Enterprise Vault archives the file and either deletes, replaces with a shortcut/ placeholder, or leaves the file in tact.

Figure 1 – Enterprise Vault and Data Insight Integration Process

Enterprise Vault and Enterprise Vault.cloud

For customers who are looking to migrate from Enterprise Vault to Enterprise Vault.cloud, the Enterprise Vault.cloud Archive Migrator tool can assist with the process. The tool is free to customers and is installed on the Enterprise Vault Server. Support is included for Enterprise Vault 9.0.5, 10.0.4, and later. Archived emails from Enterprise Vault can be easily extracted to PST format and then imported into the Enterprise Vault.cloud environment.

The tool is best for the following customer environments:

- 2TB or less of archived data in Enterprise Vault
- Environments with one or two Enterprise Vault servers

For larger or more advanced Enterprise Vault environments, it is highly recommended that the customer use an Enterprise Vault Veritas Technical Partner Program (VTPP) solution.

There are several different migration options available which include:

- Migrate user mailbox archives while maintaining mailbox folder structure
- Migrating legacy user and journal archives with no user mapping or folder structure

- Combination of above mentioned options - This will allow end users to maintain their legacy mailbox folder structure in Enterprise Vault.cloud's Personal Archive and allow the user to restore deleted emails. Legacy journal email will be isolated from Personal Archive and will reduce duplicates for discovery searches.

Figure 2 provides an overview of the process to import legacy data into Enterprise Vault.cloud.

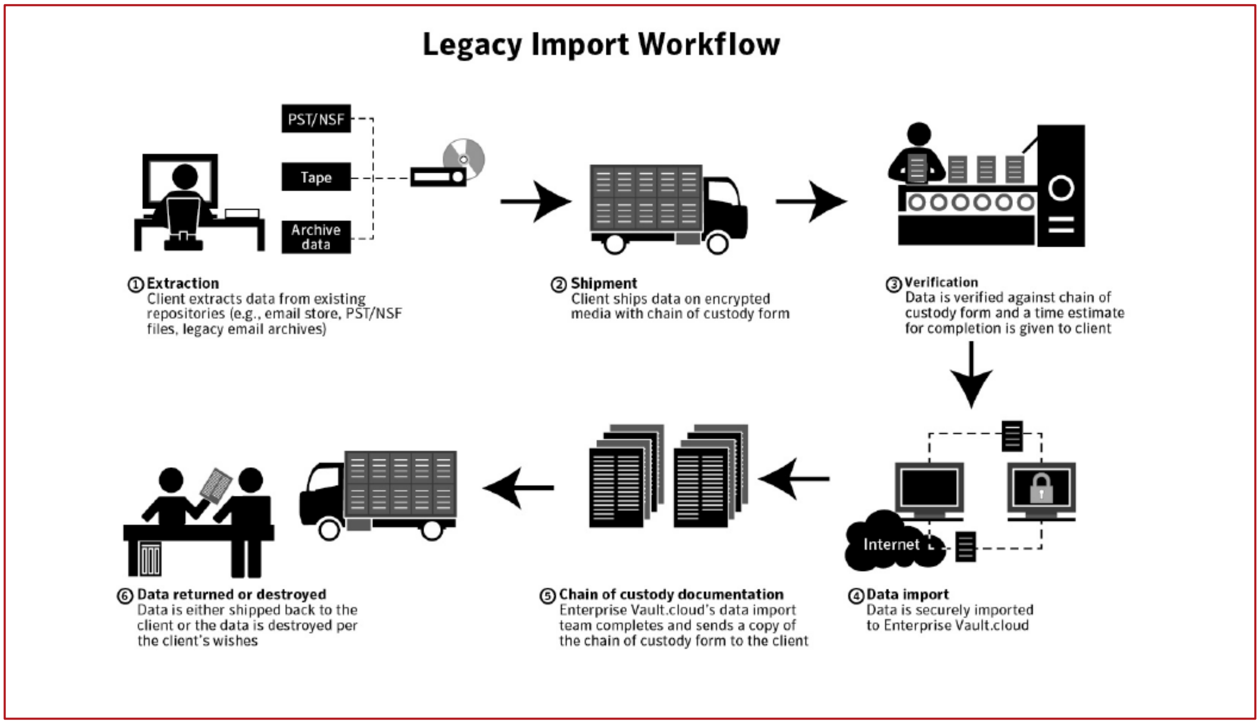
Legacy Import Workflow
PST/NSF
Tape
Archive data
① Extraction
Client extracts data from existing repositories (e.g., email store, PST/NSF files, legacy email archives)
② Shipment
Client ships data on encrypted media with chain of custody form
③ Verification
Data is verified against chain of custody form and a time estimate for completion is given to client
Internet
④ Data import
Data is securely imported to Enterprise Vault.cloud
⑤ Chain of custody documentation
Enterprise Vault.cloud's data import team completes and sends a copy of the chain of custody form to the client
⑥ Data returned or destroyed
Data is either shipped back to the client or the data is destroyed per the client's wishes

Figure 2 – Legacy Data Import Flow

Enterprise Vault and eDiscovery Platform

Starting with version 7.1.1, eDiscovery Platform (eDP) has the ability to perform searches and collections from items that have been archived with Enterprise Vault 9.0.3 and later. This integration simplifies the eDiscovery process when searching against archived content by allowing eDP to query Enterprise Vault indexes.

The eDP administrator will be required to do some minor configuration changes in order to be able to collect from Enterprise Vault. These steps include adding the Enterprise Vault Service Account (VSA) to the local administrators group on the eDP server, modify the logon credentials for the EsaEVCrawlerService service to use the VSA, install the Enterprise Vault API that matches the version of Enterprise Vault currently in use, and set up the Enterprise Vault server as a source in eDP. Figure 3 provides an overview of configuration steps.

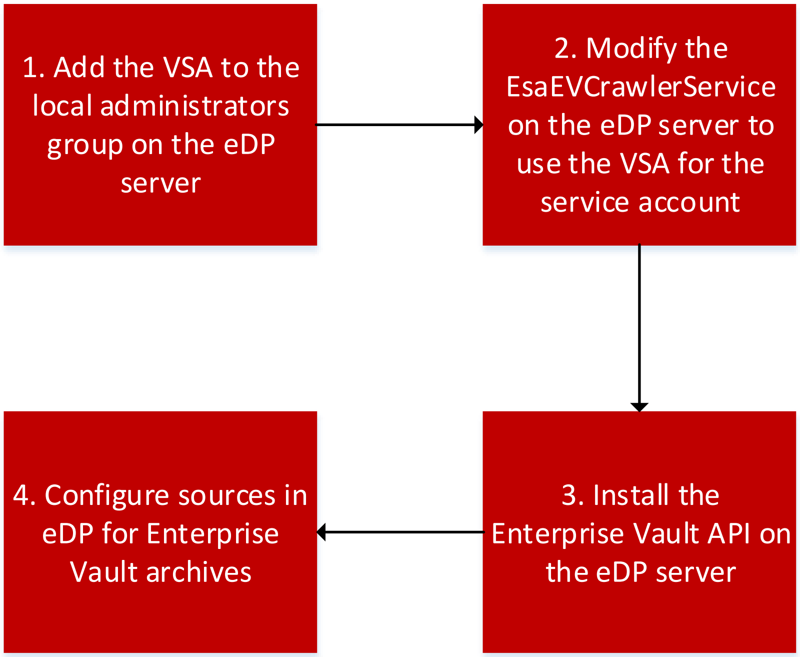
1. Add the VSA to the local administrators group on the eDP server
2. Modify the EsaEVCrawlerService on the eDP server to use the VSA for the service account
3. Install the Enterprise Vault API on the eDP server
4. Configure sources in eDP for Enterprise Vault archives

Figure 3 – Steps to integrate eDP and Enterprise Vault

Refer to https://www.veritas.com/support/en_US/article.000125192 for more information.

Enterprise Vault and Veritas Infoscale

Enterprise Vault Servers

Customers often require Enterprise Vault to be part of a highly available configuration, available in the event of a disaster, or need to replicate Enterprise Vault index volumes or Vault Store partitions to different storage platforms. Veritas Infoscale can integrate with Enterprise Vault in the following configurations:

- High Availability (HA) – Enterprise Vault can be configured in a single node cluster, an active-passive cluster, or N+M cluster configuration
- Disaster Recover (DR) – Enterprise Vault can use Information Scale components to make Enterprise Vault available at a disaster recovery location in the event of a failure in the main datacenter
- Replication – Enterprise Vault Index volumes and Vault Store partitions can be replicated using Replication to and from any storage hardware supported by Infoscale

Figure 4 provides a high-level example of clustering Enterprise Vault servers and Microsoft SQL servers with disaster recovery using Infoscale.

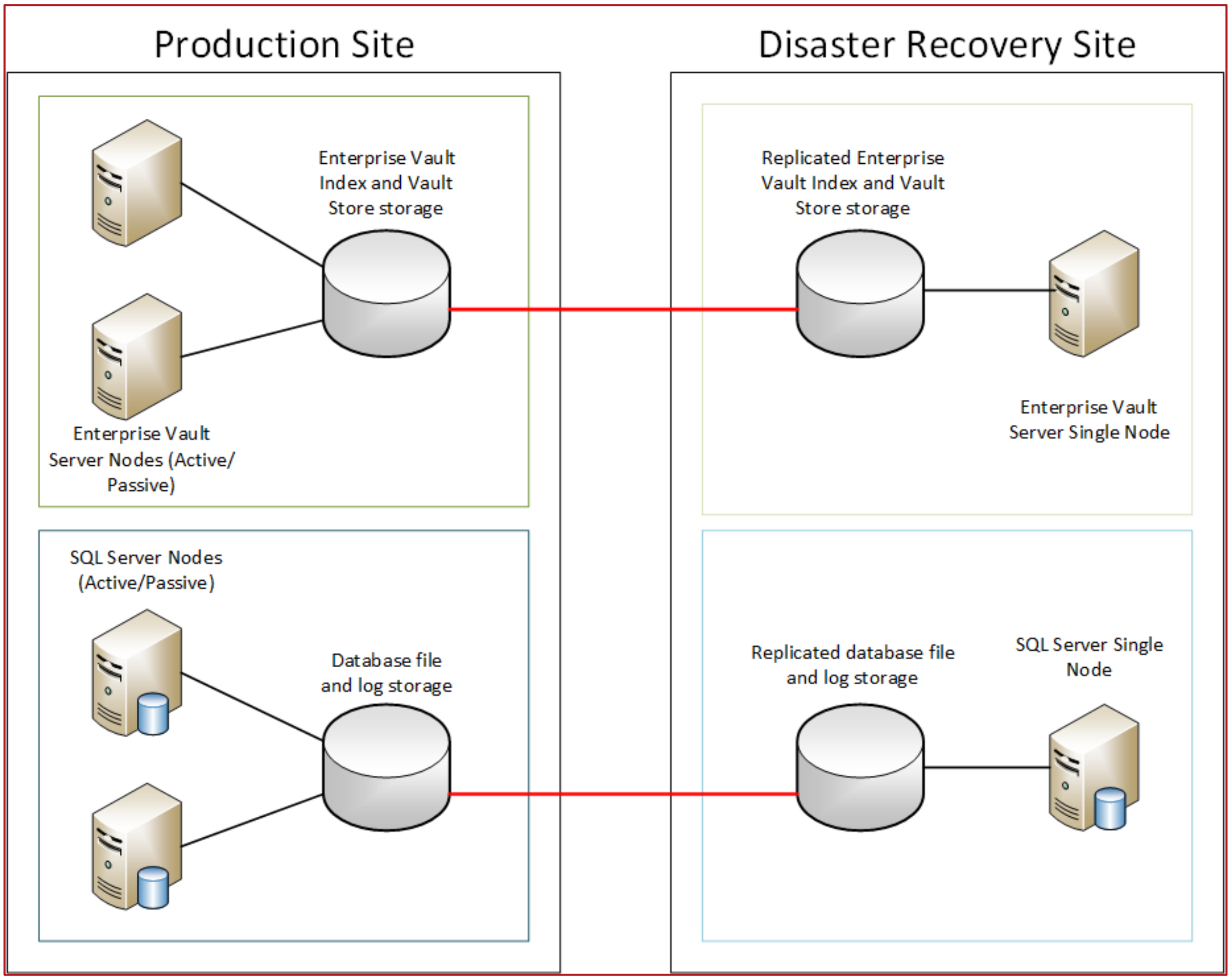
Production Site
Disaster Recovery Site
Enterprise Vault Index and Vault Store storage
Enterprise Vault Server Nodes (Active/ Passive)
Replicated Enterprise Vault Index and Vault Store storage
Enterprise Vault Server Single Node
SQL Server Nodes (Active/Passive)
Database file and log storage
Replicated database file and log storage
SQL Server Single Node

Figure 4 – Active/Passive Configuration with Disaster Recovery

File System Archiving Targets

When Enterprise Vault archives files from supported platforms, a placeholder or reparse point can be used to replace the archived file. This reparse point allows end users and applications to access the original file.

Microsoft Windows replication technologies such as distributed file system with replication (DFS-R) cannot replicate reparse points. However, Infoscale's Replication technology can properly replicate reparse points as it replicates at the volume level instead of the file level (such as how DFS-R operates). Thus, customers can confidently replicate archived file servers with Infoscale Replication.

Enterprise Vault and NetBackup

There are two main integration points with Enterprise Vault and NetBackup

- The NetBackup Enterprise Vault Agent
- Migrating archived content from Enterprise Vault to NetBackup

The NetBackup Enterprise Vault Agent

The NetBackup Enterprise Vault Agent eases the backup configuration of crucial Enterprise Vault components by removing the manual or scripted processes putting Enterprise Vault into and out of Backup Mode as well as having to keep on top of the locations of Enterprise Vault databases, Index locations, and Vault Store partition paths. Backup administrators can back up an entire Enterprise Vault environment in as little as four different policies. The NetBackup client must be installed on all Enterprise Vault and Microsoft SQL servers. The four main policies to configure are the following:

- **Main Enterprise Vault databases** – The Enterprise Vault Directory, Monitoring, Audit, and FSA Reporting databases should be backed up separately from other components and can be done so using one backup policy. The agent will automatically determine where the aforementioned databases reside.
- **Enterprise Vault Indexes** – The agent will back up all Enterprise Vault Index locations in an Enterprise Vault logical site and will automatically determine the paths to all configured Index locations. If the Enterprise Vault administrator should move or create an Index location, the agent will automatically pick up the changes.
- **Enterprise Vault Open Partitions –** The agent will automatically discover open Vault Store partitions and can also backup the Vault Store and fingerprint databases. If a Vault Store partition closes and another opens, the agent will automatically detect this change.
- **Enterprise Vault Closed and Ready Partitions –** As the data change rate on closed and ready Vault Store partitions is relatively minimal, the backup of these partitions can happen less frequently. Thus, the backup administrator can create a separate policy for the backup of these partitions. The agent will determine the state of a Vault Store partition (such as open, closed, or ready) and will automatically backup partitions that have recently changed to a closed or ready state.

For more information, please see:

https://www.veritas.com/support/en_US/article.000010873

Migrating Archived Content from Enterprise Vault to NetBackup

Archived content that resides on an Enterprise Vault server can be migrated to NetBackup to any valid storage unit. The migrated content can then be removed from the source Vault Store partition. Archived content will only restore from NetBackup when the archived content is accessed such as when a user double-clicks on a placeholder on a file system or retrieves an archived email using a search application such as Enterprise Vault Search or when an index is rebuilt for an archive.

With that said, there are times when certain types of archived content should not be migrated to NetBackup. It is highly recommended that the NetBackup Enterprise Vault migrator not be used in conjunction with email related archives (especially when migrating to tape) due to the potential sheer volume of archived content. If the Enterprise Vault environment will be performing numerous recalls of archived emails (such as using EV Browser Search/Enterprise Vault Search, Discovery Accelerator, eDiscovery Platform, exporting archived emails to PST/NSF, or verifying Vault Store consistency using the Enterprise Vault EVSVR utility), numerous restore jobs will be created on the NetBackup Master server. Index rebuilds can also cause a mass recall of content from NetBackup.

If the backup tapes that contain migrated Enterprise Vault content are not available in the tape library, the recall of the archived content will be further delayed. Lastly, if the NetBackup environment is busy with a limited number of tape drives, restores may also be delayed depending on the current amount of backup jobs running.

For more information, please see:

http://www.veritas.com/docs/000070836

About Veritas
Veritas Technologies LLC enables organizations to harness the power of their information, with solutions designed to serve the world's largest and most complex heterogeneous environments. Veritas works with 86 percent of Fortune 500 companies today, improving data availability and revealing insights to drive competitive advantage. More information is available at www.veritas.com.

For specific country offices and contact numbers, please visit our Web site: **www.veritas.com**

Veritas World Headquarters
500 East Middlefield Road
Mountain View, CA 94043 USA

+1 (650) 933 1000

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.