Enterprise Vault Whitepaper

Enterprise Vault and Microsoft Office 365

This document outlines the integration of the offsite Office 365 email service with an on-premises Enterprise Vault solution.

If you have any feedback or questions about this document please email them to **EV-TFE-Feedback@symantec.com** stating the document title.

This document applies to the following version(s) of Enterprise Vault: 10.0

Document Control

Contributors

Who	Contribution
Christopher Moreau, Senior Product Manager	Author
Andy Joyce, Director, Technical Field Enablement	Editor

Revision History

Version	Date	Changes
1.0	April 2010	Original version for Microsoft BPOS
2.0	August 2011	Updated for Office 365 and Enterprise Vault 10

Related Documents

Version	Date	Title

Table of Contents

Appendices

Overview

Microsoft Office 365 is a set of Microsoft hosted messaging and collaboration services, which includes Exchange Online (v 2010), SharePoint Online, Lync Online and Office Web Applications. Customers may wish to deploy the Microsoft Office 365 solution for their email services, thus migrating Exchange 2010 offsite, whether to reduce costs associated with running an email environment or to free resources within the corporation to perform other tasks. This document outlines the integration of the offsite Office 365 email service with an on-premises Enterprise Vault solution.

For more information on the MS Office 365 solution please see:

http://www.microsoft.com/en-us/office365/online-software.aspx#fbid=nh5laZUP0QQ

Target Audience

This document is intended for Systems Engineers, Administrators as well as individuals who leverage the Enterprise Vault 10.0 application to Journal messages for use in eDiscovery and Compliance purposes.

Why use Enterprise Vault with Office 365?

The current Office 365 offering provides an archiving feature known as Exchange Hosted Archiving. This offering provides basic archiving features allowing the user to maintain an ongoing copy of historical email for a period of time defined on a per company basis. While this feature set may service the customer with basic needs for archiving, there are instances where this offering will not cover the breadth of functionality required by more demanding use cases related to compliance, eDiscovery or corporate governance.

Table 1 shows which interactions with Microsoft Office 365 are supported by Enterprise Vault 10.0.

Enterprise Vault Feature	Support
Exchange Server Journaling	Y
PST Migration	P (Note 1)
Exchange Mailbox Archiving	N (Note 2)
Exchange Public Folder Archiving	N

Table 1 - Supported Features

Notes:

1. PST Migration will function as outlined later in this document
2. The current integration with Office 365 requires an intermediary Exchange Server to receive Journal data. There is no direct access to the cloud based Exchange server and therefore mailbox archiving is not supported at this time

The following are examples of requirements that can be provided by leveraging Enterprise Vault and Office 365 Journaling:

- **SEC 17a-4 compliant storage** – Within SEC 17A-4 there is stated the need to archive multiple copies of electronic communications for broker dealer licensed individuals on non-mutable media. Enterprise Vault supports the use of WORM media to perform this operation while many hosted solutions do not provide such functionality.

- **Retention Policy Management** – Enterprise Vault provides the ability to archive data and assign retention leveraging a policy scheme that can be configured to meet the needs of the company by the user/group or content of the data for true information management. Hosted offerings often deliver only a very high-level company-wide retention setting, which can result in over-retention or under-retention scenarios.

- **Repository of Record for Multiple Data Types** – An on-premises Enterprise Vault solution can also be used to archive, store, manage and discover other data types from on-premises file shares, SharePoint, instant messaging servers, databases as well as other information to be used for business purposes and in the eDiscovery process.

- **eDiscovery Cost Reduction and Workflow –** The eDiscovery process requires the collection of more than just email and IM received from a journal stream. Often there is a need to collect data from sources such as file shares, SharePoint sites, databases, SAP and other local resources such as desktops and laptops. Enterprise Vault provides the ability to collect, preserve and produce data natively and through advanced tool sets such as Symantec Discovery Collector and the Guidance Encase Ingest Connector to perform legal hold, review and production using Discovery Accelerator in-house. Companies continue to in-source this aspect of the eDiscovery process to reduce costs and risk. In a recent Fulbright and Jaworski survey 50-60% of respondents reported taking the preservation and collection process in-house while 62% reported performing internal investigations with internal resources.

- **Supervisory Review –** The compliance review process required by Financial Services to comply with FINRA 3010 & 3011 requires the review of data, as well as auditing of the process using a tool set which allows a hierarchy to perform proper review, escalation and auditing and tracking of the process. By leveraging the Compliance Accelerator the customer now has access to a powerful tool to meet these requirements.

Office 365 Journaling

The Office 365 Journaling feature provides a company the capability to have a Journal data stream sent to an on-premises archiving solution via use of the Exchange Journaling function. A company wishing to leverage this method is required to configure the journaling feed through Microsoft Office 365 support or configure the Journaling target via the Office 365 administration portal. The company must provide a local address to receive the data.

There are infrastructure and security configuration settings associated with the Microsoft Hosted Exchange solution, which result in some requirements in configuring Enterprise Vault for Journal Archiving.

MS Exchange envelope journal emails needs to be delivered via SMTP to an "external" journal mailbox. Thus there is a requirement for a receiving SMTP server, at this point Enterprise Vault supports extracting such data via MAPI from Exchange Server.

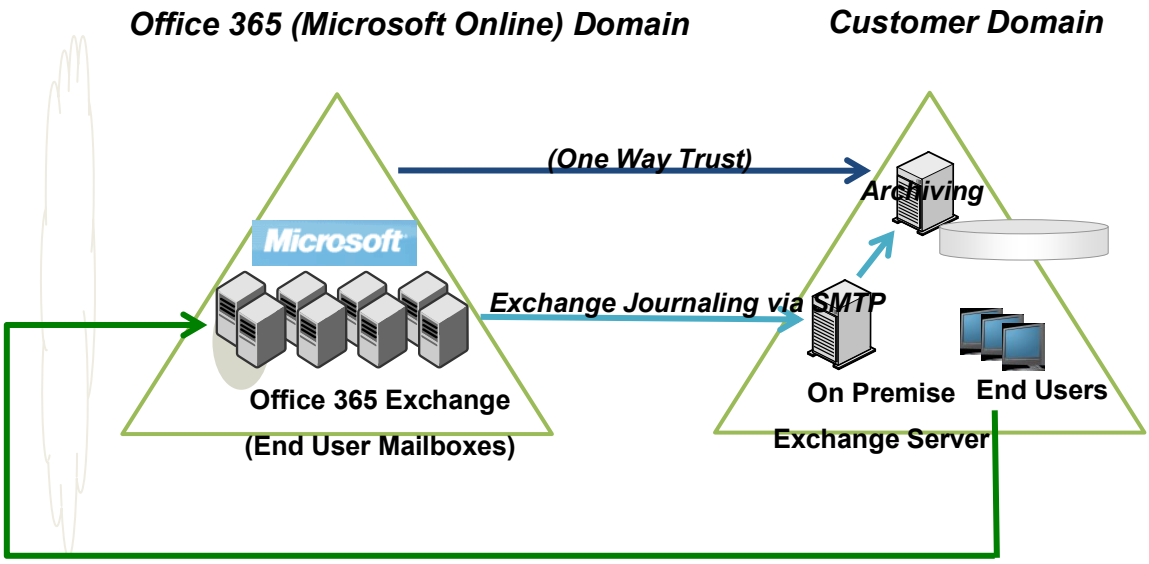

Figure 1 - *MS Exchange envelope journal email is delivered to "external" journal mailboxes, hosted in an on-premises MS Exchange server from which Enterprise Vault will extract the data using currently supported methods.*

Symantec Enterprise Vault does not provide a Message Transfer Agent at this time; therefore an intermediary MS Exchange server located on the customer premise is required to receive the data transfer from the Office 365 environment. The Enterprise Vault server then extracts the data from the Journal mailbox via an Enterprise Vault Journaling Task. All envelope information is available for indexing up to and including all recipient information (including BCC data), any information that was contained in the distribution lists from the Microsoft environment as well as all content of the message.

There are a few minor configuration settings required to process the data that are outlined in the Appendix of this document.

Note: As of Exchange 2007 the MS Exchange Journaling feature may create duplicate messages during the Journaling process depending on the number of recipients in the message. This occurs if say there are more than 1000 members in a particular distribution list or the address list contains addresses of different types, such as local mailboxes, distribution lists and external SMTP addresses. Enterprise Vault has a built in process in the Exchange Journaling task which is used to reconstitute multiple reports into single message thus only creating one entry in the archive for the particular message and thus returning only the single search result in the Discovery process.

PST Migration Limitations

The customer may wish to use the PST migration process of Enterprise Vault to ingest legacy PST data for use in the legal discovery process. The PST migration process requires connectivity to the mailbox in order to function properly and populate the proper sender information in the message when being ingested into the Enterprise Vault archive.

The PST migration builds the recipient XML looking for an SMTP address from the following properties (in this order):

PR_DEFAULT_SMTP_ADDRESS
PR_EMAIL_ADDRESS
PR_OrgEmailAddr

If these do not resolve to an SMTP address Enterprise Vault will create a MAPI session to open the Global Address Book to perform a look up on the address. This requires that there is at least one Exchange server target enabled in the EV install otherwise the process will fail.

The sender is more likely to be an issue as this is much more likely to not be an SMTP address (i.e. any internal mail dragged to a PST will have an EX address type).

The PST Migration process as of Enterprise Vault 8.0 Service Pack 4 has been extended to allow the ability to handle the scenario where the Exchange address cannot be resolved via the local Global Address list. This can be configured using the steps outlined in the Appendix of this document.

Mailbox Archiving

The current access methods provided by the Office 365 solution do not allow Enterprise Vault to access to the hosted Exchange server environment therefore mailbox archiving is not possible at this time. In the event a customer is migrating to the Microsoft Office 365 solution for hosted email from an on-premises Exchange solution where Enterprise Vault has been used to archive email from mailboxes, it is recommended to extract all mailbox archive data from the archive to PST for import to the Office 365

environment. All Journal data residing in Journaling archives can remain in the event the customer wishes to continue journaling from the Office 365 environment.

Following are some additional considerations when migrating from an on-premises Exchange solution with Enterprise Vault, to an Office 365 solution with or at a site where Enterprise Vault is not currently installed:

- **Virtual Vault -** The current version of Virtual Vault requires the presence of the mailbox and therefore will not function correctly if the mailbox is deleted from the domain after the user has been migrated to the Office 365 environment.
- **Shortcuts -** The shortcut provides reference to an internal Enterprise Vault server that is most often located within the user domain/forest. Any shortcut that has been migrated to the remote Office 365 solution will therefore attempt to connect to the internal domain, which will result in a failure to retrieve the item(s) from the archive.

Summary

In conclusion, the White Paper has focused on how to configure Enterprise Vault 10.0 to archive a Journal archiving stream from an on premises Exchange server receiving Journaled data from a hosted Microsoft Office 365 solution for use in eDiscovery and Compliance archiving. While this document is not a replacement for formal training, it will enable you and your organization to get started and will serve as a reference.

Appendix A - Journal Task Configuration Settings

1. Internal/External Recipient Markings - Since the Exchange Server is no longer local to the user domain, there is no indication that the message data is from an internal or external user (i.e. there is no correlation that Joe User login = Joe.User@company.msonline.com). This can be overcome by inserting a registry entry on the Enterprise Vault server to identify the BPOS email domain as being "internal" email traffic. This is useful for use in configuring searches and review in the Accelerator applications as well as for use in classification rules.

    a. To add internal domains using the InternalSMTPDomains registry value perform the following steps on all Enterprise Vault servers in the environment:

        i. Open the Registry Editor.
        ii. Create a string value that is called InternalSMTPDomains under the following key:

            HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\Agents

        iii. Give InternalSMTPDomains a value that specifies the required domains as a semicolon-delimited string.

        For example, you would set the value to the following to treat addresses like jld@eng.uk.eginc.com and kv@hq.eg.parentcorp.com as internal: eginc.com;eg.parentcorp.com

    b. The Journal Connector must be installed on the Enterprise Vault server for proper use of this functionality.

2. The use of the Journal stream is to capture data for use in legal discovery and compliance use cases. Since Distribution List information is contained in the message envelope, the DL expansion function will not be required on the Enterprise Vault server and thus can be disabled. To disable distribution list expansion:
    a. Open the Enterprise Vault Administration Console.
    b. Expand the contents of the left pane until the journaling policies are visible.
    c. Right-click the required policy, and then click Properties. For example:
    d. Click the Advanced tab, and then click the Expand distribution lists setting.
    e. Click Modify, and then change the value to Off.
    f. Click OK in each dialog box to save the changes that you have made.
    g. Restart the Journaling task to put the change into effect.

Appendix B - PST Configuration Settings

A registry value can be enabled which results in address resolution lookups to be bypassed. No attempt will be made to connect to an Exchange Server (even if one exists in the Enterprise Vault directory database) and the default will be to use the attribute PR_EMAIL_ADDRESS for recipients and PR_SENDER_EMAIL_ADDRESS and PR_SENT_REPRESENTING_EMAIL_ADDRESS for sender information.

1. Open the registry editor
2. Locate the following registry entry:

   HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\Storage

3. Add the following entry

   [REG_DWORD] BypassAddressLookups

   0 = OFF (Default – lookups still attempted)

   1 = ON (Bypass lookups and index the attributes per the MAPI message)

The registry value must be applied to all Enterprise Vault servers running a Storage Service, PST Migrator task or other PST migrations. Any change to the setting will require the appropriate services, tasks and migrators to be restarted.

About Symantec:

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

Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

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

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934