

Enterprise Vault 12 Whitepaper

Best Practices for Deploying SMTP Archiving

This whitepaper is intended to assist customers, partners and service providers as they plan to implement SMTP archiving.

This document applies to the following version(s) of Enterprise Vault: 12.4 and later.

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

Document Control

Contributors

Who	Contribution
Dan Strydom	Author

Revision History

Version	Date	Changes
1.0	June 2015	
2.0	June 2015	Added High Availability recommendations for Holding Folder
3.0	October 2015	Added End to End Message Tracking (Appendix F) and expanded X-Header section
4.0	November 2016	Supplementary information for archiving from Office 365
5.0	January 2018	Updated with SMTP Tracking capability
6.0	December 2018	Updated with Native decryption for Office 365
7.0	August 2020	Updates to Selective Journaling

Related Documents

Document Title	Source	Version / Date
Setting up SMTP Archiving.pdf	Product Media\Documentation	EV 12
Installing and Configuring.pdf	Product Media\Documentation	EV 12
Administrator's guide.pdf	Product Media\Documentation	EV 12
SQL Best Practice Guide	www.veritas.com/support/en_US/article.000021697	EV 12
Discovery Accelerator Best Practice Guide	www.veritas.com/support/en_US/article.100024378	EV 12
Indexing Best Practice Guide	www.veritas.com/content/support/en_US/doc/EV_BPG_VMware	EV 12

Table of Contents

Terminology	1
Introduction	1
Use cases for SMTP archiving	2
Architecture Overview.....	3
Deployment Scenarios.....	4
SMTP Journaling.....	4
How does it work?	4
Selective SMTP Journaling	4
SMTP Mailbox Journaling	6
Comparing Exchange Journaling and SMTP Journaling	7
Fan-out Factor and Address Rewriting	9
Design Considerations for SMTP Archiving.....	10
Mail Routing	10
SMTP Load Balancing and Fault Tolerance	10
Using a Hardware Network Load Balancer for SMTP Journaling.....	11
Exchange Server Back Pressure	13
Sizing	14
Additional Sizing Considerations.....	14
Typical Values Used in Sizing Estimates	15
Rule of Thumb Sizing Estimates	15
Detailed Sizing	16
Enterprise Vault SMTP Servers	16
SQL	18
Storage.....	18
Holding Folder	18
Storage Queue	19
Vault Store Partitions	19
Index.....	19
Network.....	19
SMTP Archiving for Cloud Messaging Platforms	20
Configure Journaling for Office 365	21
Configure Journaling for Gmail	22
PowerShell.....	25
X-Headers.....	26

Using X-Headers with Enterprise Vault Search	27
Using X-Headers with Discovery Accelerator	29
Monitoring and Reporting	35
Troubleshooting	38
Licensing Considerations	39

APPENDIX A – Frequently Asked Questions

APPENDIX B – Deployment Prerequisites

APPENDIX C – Configuring SMTP Journaling for Exchange Server

APPENDIX D – Creating a Send Connector with Multiple Smart Hosts in Exchange 2013

APPENDIX E – Creating a Send Connector using MX Records for Exchange 2013

APPENFIX F – End to End Message Tracking for Exchange Journal Archiving

Terminology

Term	Description
SMTP	Simple Mail Transfer Protocol
MTA	Mail Transport Agent. Transfers mail from one server to another. Referred to as “SMTP Server” in this document
SMTP Target	SMTP address recognized by Enterprise Vault server as target address
SMTP Holding Folder	Folder on Enterprise Vault server to temporarily hold incoming SMTP data in .eml format
SMTP Task	Enterprise Vault task responsible for archiving from SMTP feed
SMTP Archive	A new archive type for archiving SMTP data
SASL	Simple Authentication and Security Layer
TLS	Transport Layer Security
OSIS	Optimized Single Instance Storage
DR	Disaster Recovery
SCOM	System Center Operations Manager
Journal Report	A journal report is the message generated by the Journaling agent on a Hub Transport server and delivered to the journaling mailbox or SMTP destination
X-headers	X-headers are a standard way to add user-defined metadata to a message. X-headers are usually preserved but ignored by messaging servers and clients that don't use them.

Introduction

Enterprise Vault 11.0.1 introduces a new archiving agent that provides a simple and effective way to ingest data into the Enterprise Vault archive using the SMTP protocol. The ability to archive SMTP with Enterprise Vault has been an option of the product for many years but with 11.0.1 the architecture has been completely redesigned with greater focus on enterprise functionality and scalability.

Utilizing the SMTP protocol, Enterprise Vault can now archive any content sent to it via any application or product that supports sending email.

Use cases for SMTP archiving

Amongst other use cases SMTP archiving can be used to:

- Ingest journal email from on-premise email platforms such as Exchange Server, Lotus Domino, Sun Mail System, Zimbra directly into the archive via SMTP.
- Ingest journal emails from cloud-based email services such as Office 365, Google Mail directly into the archive via SMTP.
- Capture all metadata, such as BCC, point in time distribution list membership, journal report information etc.
- Supports supervisory sampling via Compliance Accelerator.
- Supports eDiscovery search and review capability via Discovery Accelerator.
- Ingest data from any other application capable of sending email, such as log files, voicemail, scanners, printers, fax machines, etc.
- Populate mailbox archives from the journal feed, where each user's archive is a representation of their personal journal showing Inbox and Sent items.
- Replace mail-enabled Exchange Public Folders, providing users with a more scalable shared solution.

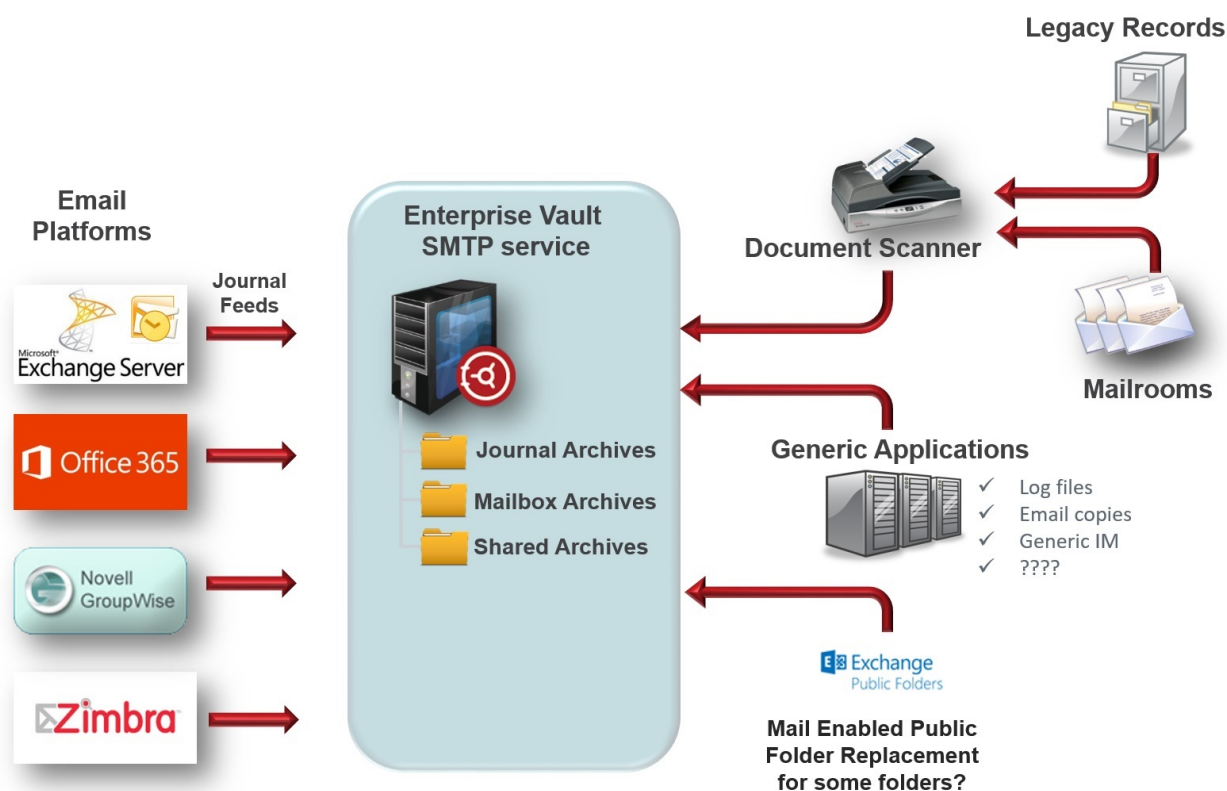


Figure 1 – Multiple content sources supported by SMTP Archiving

Architecture Overview

SMTP Archiving includes the following components:

- **SMTP Service:** Authenticates, validates and accepts SMTP traffic.
- **SMTP Archiving Task:** Ingests SMTP emails into Enterprise Vault archive based on SMTP policies and target configuration specified in the Enterprise Vault Admin Console.
- **Holding Folder:** Messages received by the SMTP Service are stored in the holding folder, before being processed by the SMTP Archiving Task.
- **SMTP Monitoring:** Monitors availability and status of the SMTP Server (MTA), SMTP Archiving task, configuration parameters and other associated resources.

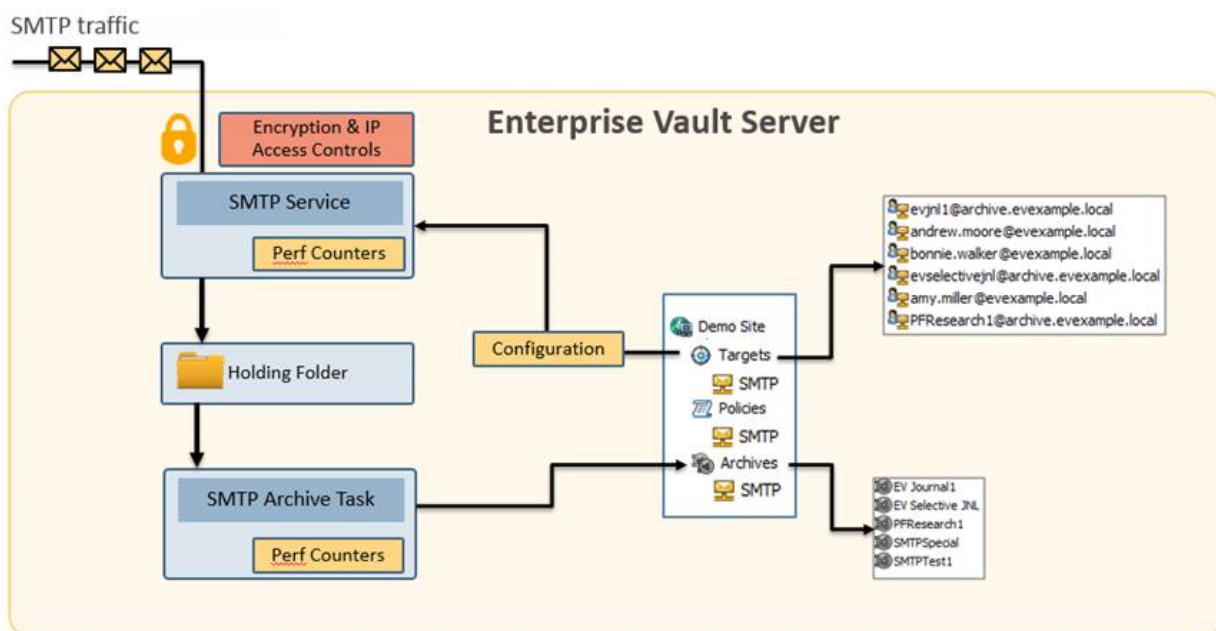


Figure 2 – SMTP Archiving Server Architecture

The journal feed from the application, typically a messaging server like Exchange or Domino, is sent to an SMTP address hosted by the Enterprise Vault SMTP Server. Each routing address is configured as a SMTP target in the Enterprise Vault Server, and is associated with an archive, which can be an existing archive of any type (Exchange, Domino, SharePoint, File, IMAP, etc) or the new SMTP archive type.

The Enterprise Vault SMTP server checks that the routing address is an SMTP target and then places the message as an .eml file in the SMTP holding folder.

The SMTP Archiving task then processes these messages from the holding folder and stores them in the associated archive.

Deployment Scenarios

With the release of Enterprise Vault 11.0.1 CHF2 there are three supported types of SMTP Archiving:

- SMTP Journaling
- Selective SMTP Journaling
- SMTP Mailbox Journaling

SMTP Journaling

In this traditional journaling method all messages that are sent to the Enterprise Vault SMTP servers are stored in one or more journal archives.

How does it work?

When the journal emails are received by the Enterprise Vault SMTP server, the SMTP Service stores them as .eml files in the Holding Folder. At this point an additional X-Header X-RCPT-TO is added to the message containing the routing email address (for example smtjournal@smtp.local, the destination set on the sending mail server).

The SMTP Archiving Task processes the .eml files in the Holding Folder. It looks at the routing email address, and compares this to the SMTP Targets configured.

Each target will have a destination archive and retention category configured. SMTP Archiving Task passes the message on to the Storage service to be archived.

Selective SMTP Journaling

Selective SMTP Journaling allows the administrator to be more specific in which email addresses will be archived.

If for example the business is only interested in archiving 5 users who perform trading duties, then a Selective SMTP Journaling archiving target can be configured to store any emails with the target address of those 5 users. Any emails sent to any of the 5 addresses can then be stored in an archive called “Trader Archives”. Or alternatively it can be configured so that each of the 5 target addresses route their journal email to their personal Enterprise Vault archives.

The above example is useful when journaling is enabled on a database level Journaling in Exchange Server, where all users on the database will be journaled to the Enterprise Vault SMTP server. The administrator is only interested in archiving the 5 users, and the remaining user’s journal stream is automatically discarded from the Enterprise Vault holding folder.

Selective SMTP Journaling can also work in conjunction with SMTP Journaling, where for example all email will be journaled to a journal archive, but additionally the Sales users will also have their journal data sent to a Sales archive with a different retention period.

How does it work?

Selective Journal Archiving configures the SMTP Archiving task to search all of the sender and recipient fields (X-RCPT-TO, To, CC, BCC, From, Sender) in each message.

To optimize performance for SMTP Journaling, ensure that this advanced site setting is set to Non-selective. This setting applies to SMTP Archiving only.

If you use SMTP provisioning, ensure that this advanced site setting is set to Inclusive or Exclusive. When you create the first SMTP provisioning group, Enterprise Vault automatically selects Inclusive for you. However, if you subsequently change the setting, Enterprise Vault does not update it.

Supported values:

- Non-selective (default). Match recipients in X-RCPT-TO field only.
- Inclusive. Match SMTP target addresses in all of the sender and recipient fields (X-RCPT-TO, To, CC, BCC, From, Sender). A copy of the message may be stored in multiple archives.
- Exclusive. Match SMTP target addresses in all of the sender and recipient fields except X-RCPT-TO and store messages in archives associated with matching selective target addresses. If no selective target address matches the message recipient fields (To, CC, BCC, From, Sender), then the email is stored in the archive associated with the target SMTP address in the X-RCPT-TO field.

Similar to the process described in the SMTP Journal archiving section, the SMTP server will add the X-RCPT-TO header to the email. The SMTP Archiving Task processes the .eml files in the Holding Folder. The task looks at the routing email address the SMTP Service stored in the X-header, and compares this to the SMTP Targets configured.

At this point the process changes as the Selective Journal Archiving setting is enabled. Once enabled, this setting will allow the SMTP Archiving Task to also investigate the To, CC, BCC, From and Sender headers to determine a match for any of the configured target addresses.

For each target address where there is a match, then the message will be archived to the appropriate archive, with the retention category associated with that target address.

The journal address where the messaging server will be sending the emails to must be configured as a target (for example smtpjournal@evsmtp.local) in order for the SMTP service to accept the email. If only the selective journal address targets are required for archiving, then archiving for the journal target address can be disabled (Figure 3). If left enabled, the email will be stored in both the journal archive, and the archive specified by the selective target address.

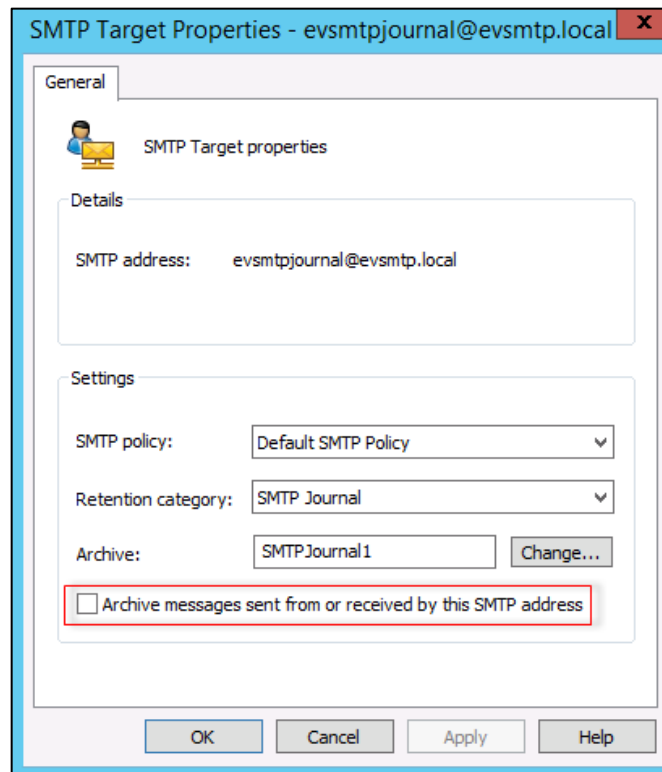


Figure 3 – Selecting whether to archive an SMTP target address

If disabled, only the selective archive targets will be archived, and the emails that do not match any of the target addresses will be deleted from the holding folder.

In Selective SMTP Journaling and SMTP Mailbox Journaling, all messages that contain a target address in a recipient field are stored in the Inbox of the archive. If a target address is found in the Sender or From fields, the message is stored in the Sent Items folder. If a target address is both the sender and recipient of a message, the message is stored in both the Inbox and the Sent Items folder of the archive.

Enterprise Vault 11.0.1 CHF2 and later also supports archiving of target addresses where the address were part of a distribution list. The distribution list must be expanded by the sending messaging server prior to archiving. For Exchange Server this will be done automatically.

Important Note: Enabling Selective Journaling will result in an estimated reduction of 25% in archiving performance due to the additional investigation performed on every email. In benchmark tests where 5,000 selective targets were configured the server archiving throughput was reduced by 50%. See Table 3 to work out required number of servers and CPU cores.

SMTP Mailbox Journaling

SMTP Mailbox Journaling is aimed at providing a solution for end users where they can see a copy of all of their sent and received messages in a personal journal archive. The end user will have access to an archive with a folder Inbox (for all messages they received) and a folder Sent Items (for everything they've sent).

How does it work?

Mailbox SMTP Journaling works in a very similar way to Selective SMTP journaling. The key difference is that for Mailbox Journaling there is a 1:1 mapping of the end user's journal archive with their target address, where with Selective Journaling several target addresses can be associated with a single archive (Sales Department for example).

Note: Configuring SMTP Mailbox journaling for a large number of users will result in a larger index footprint, as there will be a high degree of duplication of messages in the archives (similar to standard Exchange Mailbox archives). The messages will be single instanced, but there will still be more growth in index volumes and SQL Vault Store databases. Also note that only target addresses configured will be archived, if a user has multiple aliases addresses they should also be configured as targets.

For details on how to configure Selective and Mailbox Journaling refer to the "Setting Up SMTP Archiving.pdf" document (referenced documents).

Comparing Exchange Journaling and SMTP Journaling

For customers that require Exchange Journaling the only option prior to SMTP Archiving was to send journal email to journal mailboxes, hosted on Exchange Mailbox servers. Enterprise Vault then continuously collects the journal data with Exchange Journaling tasks.

SMTP Archiving provides an alternative approach, whereby Exchange server sends the data directly to Enterprise Vault via an Exchange Send Connector, without the need for journal email to go into a dedicated journal mailbox first. Performing Journaling in this manner greatly reduces complexity and architecture requirements, resulting in a reduction in total cost of ownership.

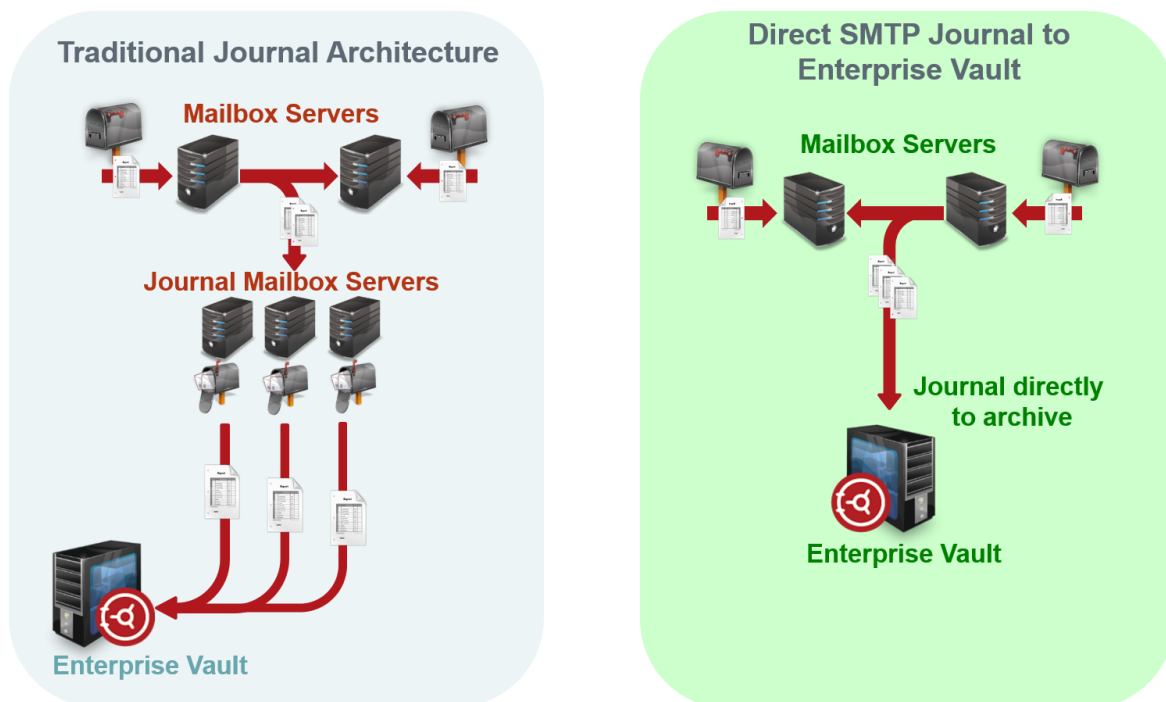


Figure 4 – Traditional Journal architecture vs. Direct SMTP Journaling

A benefit of SMTP Archiving is that it provides the ability to remove the large amount of duplicate email when journaling to multiple mailboxes (known as the fan-out factor). See section on Fan-out and Address Rewriting.

Table 1 summarizes the differences between Exchange Journal Archiving and SMTP Archiving.

Capability	Exchange Journal Archiving	SMTP Archiving
Single Instance Storage	Yes	Yes
Support for cloud-based messaging systems	No	Yes
Eliminate fan-out	Yes – via 3 rd party add-on	Yes
Suitable for geographically dispersed environments with slower network links (SMTP vs MAPI)	No	Yes
Classification	Yes – via DCS and customer filter	Yes
Journal to Mailbox Archives	No	Yes
Journal to non-Journal Archives	No	Yes
Index Footprint	12%	6-9%
Add additional Index attributes	Yes – via Custom Filter	Yes – via X-Headers
DL Member search using display name	Yes	Yes – With Journal Report and Custodian Manager ¹
DL Member search using SMTP address	Yes	Yes – With Journal Report
Support for Exchange Journal Decryption	Yes	Yes
Selective Journaling	Yes – Via Custom Filter	Yes
Support supervision via Compliance Accelerator	Yes	Yes
Support for Discovery Accelerator	Yes	Yes
Support for eDiscovery Platform, powered by Clearwell	Yes	Yes

Table 1 – Comparison of Exchange Journal Archiving and SMTP Archiving

¹ Otherwise search on DL only

Fan-out Factor and Address Rewriting

The term “fan-out” refers to the duplicate journal emails generated by Exchange Server when more than one journal destination (Journal mailbox or SMTP Journal recipient) is configured in Exchange Server.

Fan-out occurs when a message is sent to 2 or more users, and the individual recipients (or their associated Exchange databases) are configured to journal to different journal mailboxes or different SMTP journal addresses. The Exchange server will then send a copy of the journal message to both journal locations, thereby creating duplicate items. The higher the number of journal mailboxes/addresses, the higher the number of duplicate messages.

For larger customers the effect can be substantial:

- For one journal destination fan-out = 1.00 x # of unique messages
- For two journal destinations fan-out = 1.75 x # of unique messages
- For three journal destinations fan-out = 2.11 x # of unique messages
- For four journal mailboxes fan-out = 2.73 x # of unique messages.

Enterprise Vault is able to de-duplicate these items at a storage level by using its Optimized Single Instance Storage engine. However the additional load on the Exchange Servers and the Enterprise Vault servers to process the extra messages, and the extra storage required for indexing and SQL databases is still undesirable.

Enterprise Vault 11.0.1 CHF2 and later versions is able to remove the fan-out using a feature known as Address Rewriting (Figure 5).

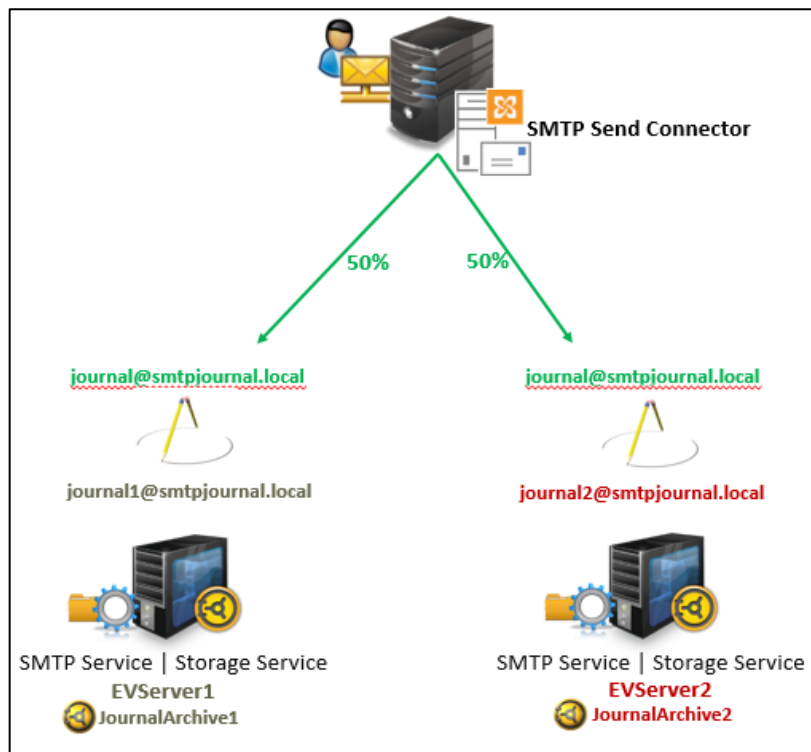


Figure 5 – Address Rewriting

Address rewriting allows the Exchange administrator to specify a single journal address for the whole environment, whether configured on a number of databases or at the transport level. The Exchange Send Connector then load balances (using either multiple Smart Host entries or MX records) the journal stream to the Enterprise Vault servers.

Enterprise Vault will accept the journal traffic on any SMTP Server. The address rewriting feature will then rewrite the X-RCPT-TO address to a target address of the local archive (journal1@smtpjournal.local or journal2@smtpjournal.local in the example).

The original item remains unchanged, only the journal envelope address is modified.

The benefit of this feature can be summarized as follows:

- Less strain on Exchange servers handling the duplicate items
- Smaller Enterprise Vault server footprint as there are less messages to process
- Smaller Index volumes
- Smaller SQL Vault Store databases
- No duplicate results in Discovery and Compliance Accelerator

Existing Exchange Journaling customers with multiple Journal mailboxes considering a migration to SMTP Archiving can email ev-tfe@symantec.com to obtain an estimate number of messages with fan-out removed. Please include the number of messages archived per day (as reported by Enterprise Vault), the number of users in the organization and the number of journal mailboxes.

Design Considerations for SMTP Archiving

This section will cover how to design and configure SMTP archiving for Exchange Server journaling. The design approach also applies to other on premise email platforms, such as Lotus Domino, Zimbra, and Novell GroupWise.

Mail Routing

One of the most important aspects of an SMTP archiving design is how the journal email will be routed from the Exchange server to the Enterprise Vault SMTP server. The high availability aspect of this design is crucial – any network or server outage will cause build-up on the Exchange Connector queues.

SMTP Load Balancing and Fault Tolerance

MX records, smart host connector load balancing or a hardware load balancer is used to determine which EV SMTP server the message will be sent to.

A common misconception is that traffic can be load balanced by creating two Send Connectors with the same cost. When two connectors exist, Exchange will simply choose the one with the alphanumerically lower name – it will not load balance outgoing emails.

The least complicated and most secure method is to use multiple smart host entries in the Exchange Send Connector. This method does not require any new DNS zones, or creation of MX records in DNS. It also allows the administrator to select authentication and encryption methods on the connector, where MX records do not.

If you have more than one smart host configured in a Send Connector, Exchange will use them in a rotating order so that the smart hosts receive mail equally. High availability is also accomplished with this method – if one host is not available the connector will use the next host.

See Appendix D for detailed steps on how to configure multiple smart hosts.

As an alternative to the Smart Hosts configuration described above, MX records can be used to provide load balancing and fault tolerance. MX records require more configuration than smart hosts, and do not provide the option to encrypt messages.

See Appendix E for detailed steps how to configure MX records for SMTP archiving.

Using a Hardware Network Load Balancer for SMTP Journaling

Another alternative is to use a hardware load balancer. Hardware load balancers are highly configurable, intelligent devices capable of routing SMTP email based on a number of factors.

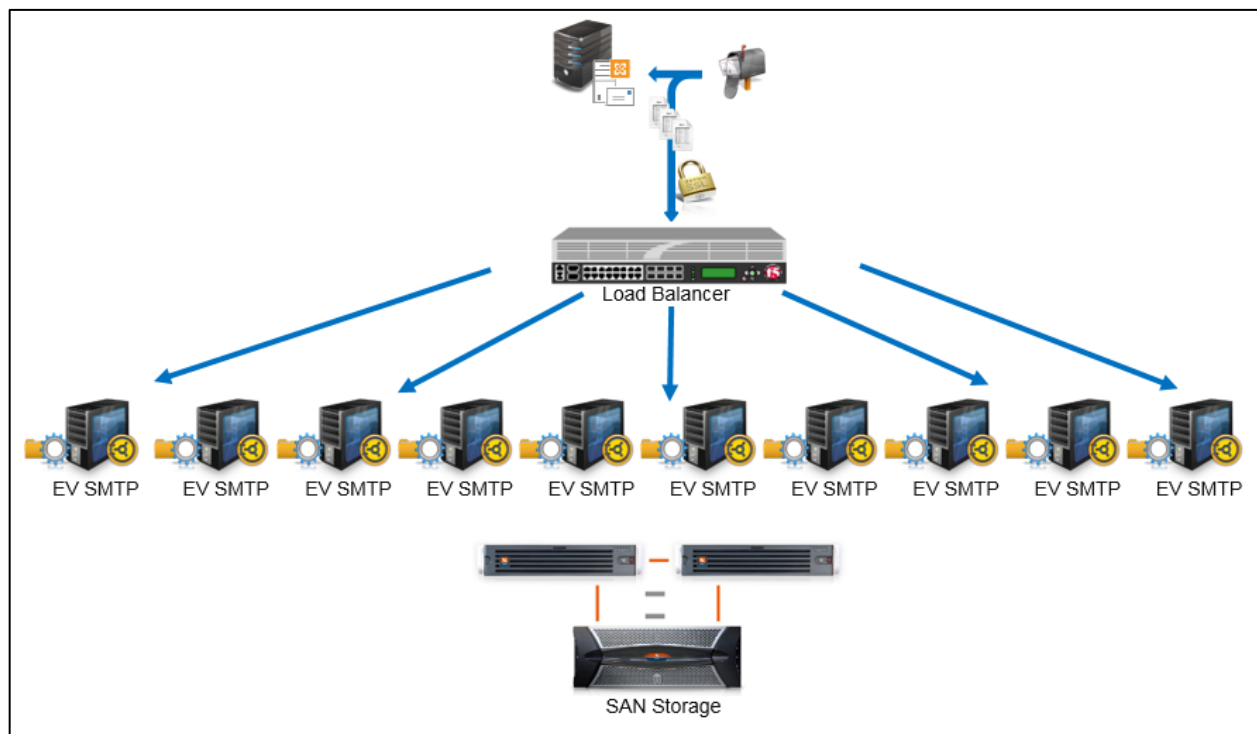


Figure 6 – Typical Hardware Load Balancer deployment

Advanced monitoring and health probes can be used to determine the most suitable SMTP host, in addition to configurable metrics such as weights and a choice of load balancing algorithms.

Table 2 compares the different technologies discussed in this section.

Method	Advantages	Disadvantages
Multiple Smart Hosts in Send Connector	No Cost Simple and quick configuration	Failed hosts that will remain down for longer periods of time will have to be manually removed No health checks
DNS Equal Preference MX Records	No Cost	More configuration – Additional DNS Zone, MX Record entries Failed servers that will remain down for longer periods of time will have to be manually removed No health checks
Hardware Load Balancer	Additional statistics and reporting Health monitoring probes Selection of load balancing algorithms Ability to direct % of traffic to certain hosts	Additional cost

Table 2 – Comparison of Load Balancing Technologies

The following guidelines are recommended:

- Use multiple smart hosts in the Exchange Send Connector to provide load balancing and fault tolerance.
- If an existing hardware load balancer is available on the internal network it would provide an optimal solution for load balancing and fault tolerance.
- Ensure that the Enterprise Vault SMTP servers are configured to accept traffic from the Exchange servers that are configured to use the Exchange Send Connector (Figure 7).

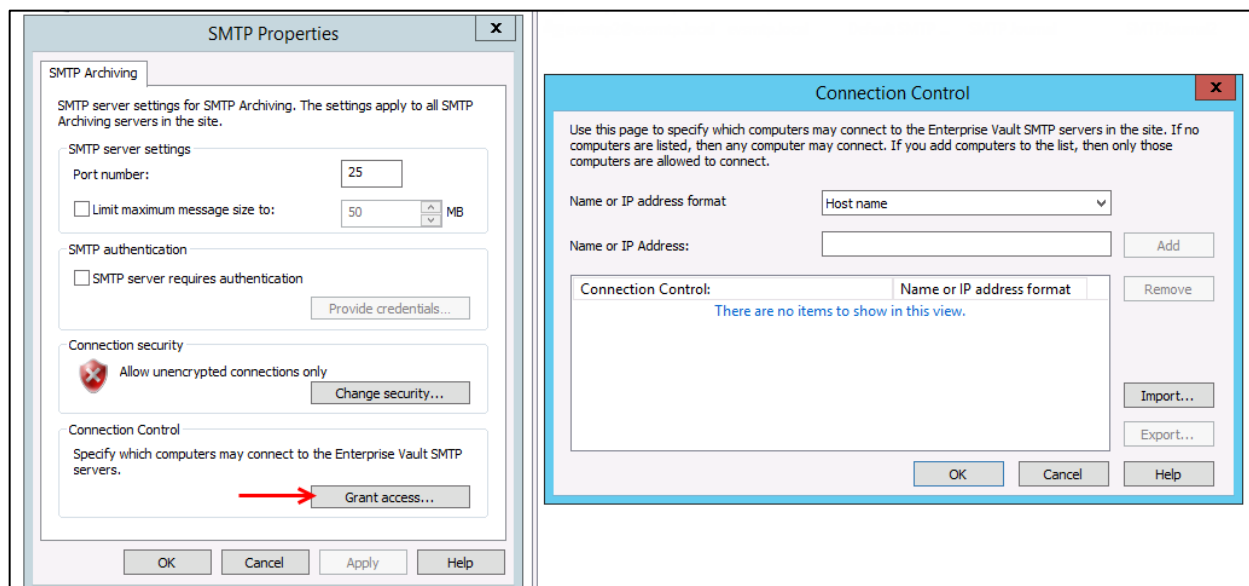


Figure 7 – Control which servers the SMTP server is allowed to receive mail from

Exchange Server Back Pressure

The importance of having high availability in the SMTP archiving solution becomes obvious when faced with rapidly growing mail queues on an Exchange Server. Having fault tolerant means of off-loading the journal report to another Enterprise Vault SMTP server is a must have in any SMTP archiving design.

Depending on the size of the queue and the load on the Exchange server, Exchange will start applying “Back Pressure”², a mechanism to throttle connections and resources to prevent the server from being overwhelmed. Amongst other factors back pressure monitors the free space on the disk queue location, the number of uncommitted queue transactions in memory and the number of messages in the submission queue.

If the Exchange server message queue location is left in the default location (%ExchangeInstallPath%TransportRoles\data\Queue) and there is an outage in either the message route (name resolution issue, network outage, hardware load balancer failure), or no Enterprise Vault SMTP server is available to receive the journal stream, then it is only a matter of time before back pressure will take effect.

It is recommended that the mail queue directory on the Exchange Server is moved to a location with appropriate disk space, and that appropriate monitoring alerts are configured.

² For more information on this Exchange 2013 feature see article [https://technet.microsoft.com/en-us/library/bb201658\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/bb201658(v=exchg.150).aspx)

Sizing

Sizing for Enterprise Vault is generally only done up to 3 years ahead in time. The benchmarks, estimates and assumptions on which the sizing is based are unlikely to be valid beyond that time. Additionally, server, storage and software technology is also likely to change in 3 years' time.

When sizing an SMTP archiving solution there are three main outputs:

Enterprise Vault Servers: How many EV servers do I need to cope with the daily influx of journal email? Where should these servers be located, and what specification servers are required? Will the servers be able to keep up with the load during business hours if one server fails? Will these servers be able to keep up in three years' time? In addition to SMTP archiving, are there any other requirements such as Discovery or Compliance Accelerator?

Storage: How much storage is required for the Vault Store Partitions, Index, SQL databases, Holding Folder and Storage Queue today, and how much is required in 3 years' time?

SQL Requirements: How many CPU cores and memory will be required for the SQL instance to support the solution for 3 years? What is the size of the databases likely to be?

Additional Sizing Considerations

The main factors which need to be considered when sizing for SMTP archiving are:

- How many journal emails will be received on a daily basis?
- What are the core business hours where the majority of emails will be received? Are there any email servers in different geographic locations that will send journal email while the EV server(s) is being backed up or under maintenance?
- If there are any remote email servers, is the available bandwidth sufficient to cope with the journaling traffic?
- How is the message volume likely to change over the next 3 years? Is the average message size likely to increase? Will there be more users on the Exchange servers? Is attachment sizes likely to grow? Will there be an increase in email activity such as email marketing campaigns?
- Will there be any additional SMTP archiving required, such as Instant Messaging, Fax, Scanners, etc.?
- How often will searches be performed on the data? If the business requires regular searches then it may be necessary to add additional resource to support the index volume (faster storage), increased memory and additional CPU cores to the EV server to ensure the ingestion performance does not suffer. See *Index Best Practices Whitepaper* and *Discovery Accelerator Best Practices* for more information (referenced documents).
- Between backup and maintenance schedules, how much time will the Enterprise Vault server have for archiving? The server can continue to receive SMTP emails while the Enterprise Vault servers are unavailable, but a large buildup in the holding folder should be avoided where possible.

Typical Values Used in Sizing Estimates

The following values are considered typical for sizing SMTP archiving.

- The average size of a Microsoft Exchange message is around 75KB.
- A typical end user sends and receives between 70 and 100 emails per workday.
- The sizing estimates are usually based on an organization having 260 work days per year.
- For SMTP Journaling the Full index size is typically around 9% of the size of the original messages. Note that this value is lower than Exchange Journaling which is calculated at 12%. MAPI messages contain unique message fields that grow the index “dictionary”, where EML files do not contain these properties.
- An Enterprise Vault Server with 8 CPU Cores and 32GB RAM can archive 120,000 items per hour

Rule of Thumb Sizing Estimates

Using the values described in the previous section a very simple rule of thumb calculation can be provided to assist with high-level sizing. Note that this estimate does not include any growth of message volume or size, and cannot be relied upon to design a solution. Veritas consultants and certified partners have access to a sizing estimator tool that can be used to provide detailed sizing estimates.

Rule of Thumb 1: A single 8-core CPU Enterprise Vault Server with SMTP, Storage and Index locally can support SMTP archiving for approximately 12,000 users (or 1,200,000 messages per day)

This estimate is based on:

- 75KB average message sizes
- A typical mix of messages with and without attachments
- A single Journal SMTP address (no fan-out)
- Virtual server with 8 dedicated CPU cores and 32GB reserved memory
- Non-selective SMTP Journaling of 120,000 items per hour, processed and archived within a 10 hour window
- **Important Note:** A single EV SMTP server will not provide high availability. It is recommended that a further EV SMTP host is added to provide failover, and the sending email application is configured to load balance across the two servers.

Rule of Thumb 2: Storage required for 12,000 users for 1 year of SMTP Archiving:

- 12TB Vault Store
- 2TB Index Volume (Full Indexing)
- 170GB SQL
- 400GB Holding Folder

Based on:

- 1,200,000 messages a day
- Average message size of 75KB
- A typical mix of messages with and without attachments
- 260 work days a year
- Note that these sizing estimates are only indicative figures, actual numbers will vary depending on message type and content.

Detailed Sizing

This section will cover each component design in detail. It is recommended that the services of a Veritas or Certified Partner consultant is engaged to provide a detailed design with 3 year sizing estimates.

Enterprise Vault SMTP Servers

According to Veritas benchmarks an optimally configured Enterprise Vault server with SMTP, Storage and Index services locally can obtain the following throughput:

CPU Cores	8-core	8-core	16-core	16-core
Average Message Size	125KB	70KB	125KB	70KB
Archived items per hour	65,000	120,000	125,000	165,000

Table 3 – Benchmark Performance for 8-core and 16-core servers

Performance testing showed that splitting SMTP Services from Storage (in other words having a dedicated Enterprise Vault SMTP server, and Storage and Indexing Services on a different Enterprise Vault server) is not the most effective way of utilizing server hardware. Instead an “All-in-one” building block approach with SMTP, Storage, and Indexing on the same server provides a more cost effective way of scaling out.

The following process should be followed to determine how many Enterprise Vault servers are required:

Determine how many journal emails are expected per day.

- Existing Exchange Journal Archiving customers can monitor their Enterprise Vault reports to determine the number of items archived per day (bear in mind reduction possible due to removal of the fan-out factor)
- New customers can use message tracking or performance counters. There are a number of 3rd party tools and PowerShell scripts that can be used to extract message statistics.
- Alternatively a temporary journal mailbox can be created, and journaling for one typical mailbox database configured to journal to that mailbox for a 24 hour period. This will give an indication that can then be extrapolated for the total number of users. Ensure there is sufficient disk space on the mailbox database for this test, and that the mailbox quota is removed from the journal mailbox.

- Note that SMTP gateway statistic cannot be used to determine the number of expected journal messages, as that will only measure the number of email leaving and entering the organization.
- Determine the current average message size of messages
 - Use either Enterprise Vault reports, 3rd party tools or PowerShell scripts provided by Microsoft to determine the average message size in the organization.

The next step is to determine which CPU profile is required per server to archive the number of messages, with consideration to the message size (as can be seen from Table 3 the larger the average message, the lower the archiving throughput).

A very important factor at this point is the amount of time in which the journal data will be received by the SMTP Service, and archived on the Enterprise Vault server. Typically it is assumed that 90% of email is received during the 10 hour business period, and it is important that there is no large build-up of queues on the Exchange Server during this time (as described in the Exchange back pressure section).

The next step is to divide the estimated number of messages per day by the amount of hours in which it will need to be archived in. The result will be the number of messages that needs to be archived per hour.

For example 1,200,000 messages a day / 10 hours = 120,000 per hour. If the average message size is 75KB, then that is a perfect fit for a single 8-core CPU server throughput (120,000 items per hour from Table 3).

If for example it is estimated that 5,000,000 messages will be journaled per day: 5,000,000 / 10 hours = 500,000 per hour. The 16-core profile server can handle 165,000 per hour; therefore we estimate we will need at least 3 x 16-core Enterprise Vault servers.

Important Note: Both example calculations only reflect the minimum number of servers. The design must cater for failover - without an SMTP server to off-load the journal data to, the email will queue on the Exchange Server attempting to use the Send Connector.

Therefore in both examples at least one additional server should be added to allow for any outage, and the sending Exchange Server configured to load balance across the servers.

If required, an additional number of Enterprise Vault SMTP servers can be added at a Disaster Recovery data center. In the event of losing the primary site the Exchange Send Connector can be updated to use the smart host addresses for the Enterprise Vault SMTP servers in the failover site. Alternatively, MX records can be configured with a higher priority to deliver mail to failover hosts.

Optionally, customers can also use clustering services to make the Enterprise Vault SMTP server highly available. In which case, the SMTP holding folder needs to be configured on the shared storage location accessible from all the clustering nodes.

Another factor that will impact the number of Enterprise Vault server is whether SMTP emails are encrypted. Benchmark tests showed that the archiving throughput on a single server with SMTP and Storage services reduced by 50%. Allow for additional servers to counter this reduction.

SQL

The formulas to calculate the SQL Database sizes are set out in the Enterprise Vault 11.0 SQL Best Practices Guide (referenced documents), and are also available in the Sizing Estimator tool.

For SMTP journal, archiving do not use archives that are enabled for Fast Browsing, as this will grow the Vault Store database unnecessarily.

For SMTP Mailbox Journaling where end users will regularly access and search their journal archives the archive can be enabled for Fast Browsing. To determine the additional growth in the Vault Store database caused by metadata-enabled archives, see Vault Store database calculation section in Chapter 3 of the SQL Best Practices Guide.

To determine the amount of CPU cores and memory required for the SQL Instance used by the Enterprise Vault SMTP servers, use the following rule of thumb:

- 8 CPU cores and 16GB RAM for every 8 Enterprise Vault SMTP servers
- Additional for resources may be needed for SQL Reporting, Discovery Accelerator or Compliance Accelerator.

Storage

The following section will provide guidelines for sizing storage components used by SMTP archiving.

Holding Folder

The SMTP Holding folder should be on a fast (minimum 300 IOPS), resilient storage device such as a SAN. The folder should not be on a system drive, or a drive that is shared by other processes. If possible the drive should be replicated to an alternative location as a failsafe measure in the event of a local storage device failure. Supported examples of making the folder highly available include:

- Windows Distributed File System (DFS)
- Storage-based replication
- Veritas Volume Replicator
- 3rd party replication software

The holding folder can be replicated either to another Enterprise Vault server or File Server.

Security of the holding folder should be carefully considered. This folder will contain .EML files from the journal that can potentially be read while in the processes of being archived. Ensure only the Vault Service Account has access to this folder, and that other server administrator accounts do not inherit permissions.

Folders created in the holding folder are organized by the time at which the message was placed in the folder. For example:

```
Mail Root (Holding folder)
  26 (day of month)
    15 (hour)
      30 (min)
        5cd6a8ba01cc51dd00000001.eml (actual email)
```

Any email that cannot be archived will be stored in a "Failed" folder. An error will be logged in the eventlog containing the reason why the message failed to archive.

Ensure that the holding folder is excluded (along with the other recommended Enterprise Vault storage locations) from both real-time and scheduled anti-virus scans.

The default behavior is to delete any messages from the holding folder that do not have a configured target email address. In the advanced SMTP tab of the Site properties the configuration can be changed to move items to a folder *NoMatchingTarget* instead.

Build-up of email in the holding folder should be avoided – the local storage and indexing services should be capable of keeping up with the workload. Adding more CPU cores to the Enterprise server is likely to improve archiving performance if required.

It is recommended that the holding folder is sized to allow for 5 days of build-up. Calculate the amount of email expected to be received on the server, multiply by the average message size, multiply by 5 and convert to the value to GB.

The reason why the recommendation is more than 1 day is to allow for any outage on the Enterprise Vault archiving processes. As previously stated it's important to avoid queues on the sending messaging server, as that can directly impact end users.

The Enterprise Vault SMTP service operates completely independently of the Admin, Directory and Storage services on the computer, and is still able to receive email while the Enterprise Vault core services are unavailable (useful when performing upgrades or maintenance).

Storage Queue

It is recommended that the Storage Queue feature is used for SMTP Archiving. Select the “Yes, in Storage Queue” option on the Vault Store that contains the SMTP archive. For more details on sizing and configuring the Storage Queue refer to the Administrators Guide.

Vault Store Partitions

Estimating Vault Store Partitions is normally done using the Sizing Estimator Tool, as it is a very time consuming process. The formula is discussed in detail in the Enterprise Vault 11.0 Performance Guide (SMTP archiving section).

Index

Indexes sizes are calculated at 9% of the original message volume archived.

Indexing Type	% size of original data
Brief	2%
Full	6-9%

Table 4 – Index volume sizing

Index volumes should reside on fast storage such as a SAN, especially if regular, large eDiscovery searches are expected. Consult the Enterprise Vault Indexing Best Practice guide for more information.

Network

Enabling Exchange Journaling in an environment with Exchange Servers in geographically distributed locations is likely to have an impact on the wide area network. The impact on each location should be

carefully considered, so too the overall SMTP design (centralized or localized instances of Enterprise Vault). If using unencrypted SMTP traffic, WAN Accelerators can be used to shape and optimize mail flow.

Further network considerations are outlined in the Enterprise Vault 12 Performance guide.

SMTP Archiving for Cloud Messaging Platforms

In this scenario, customers using any cloud based messaging platform and looking to keep a copy of their emails on premise, can configure their cloud messaging platform to send a copy of the journal feed to an SMTP address hosted by Enterprise Vault SMTP server as depicted in Figure 8.

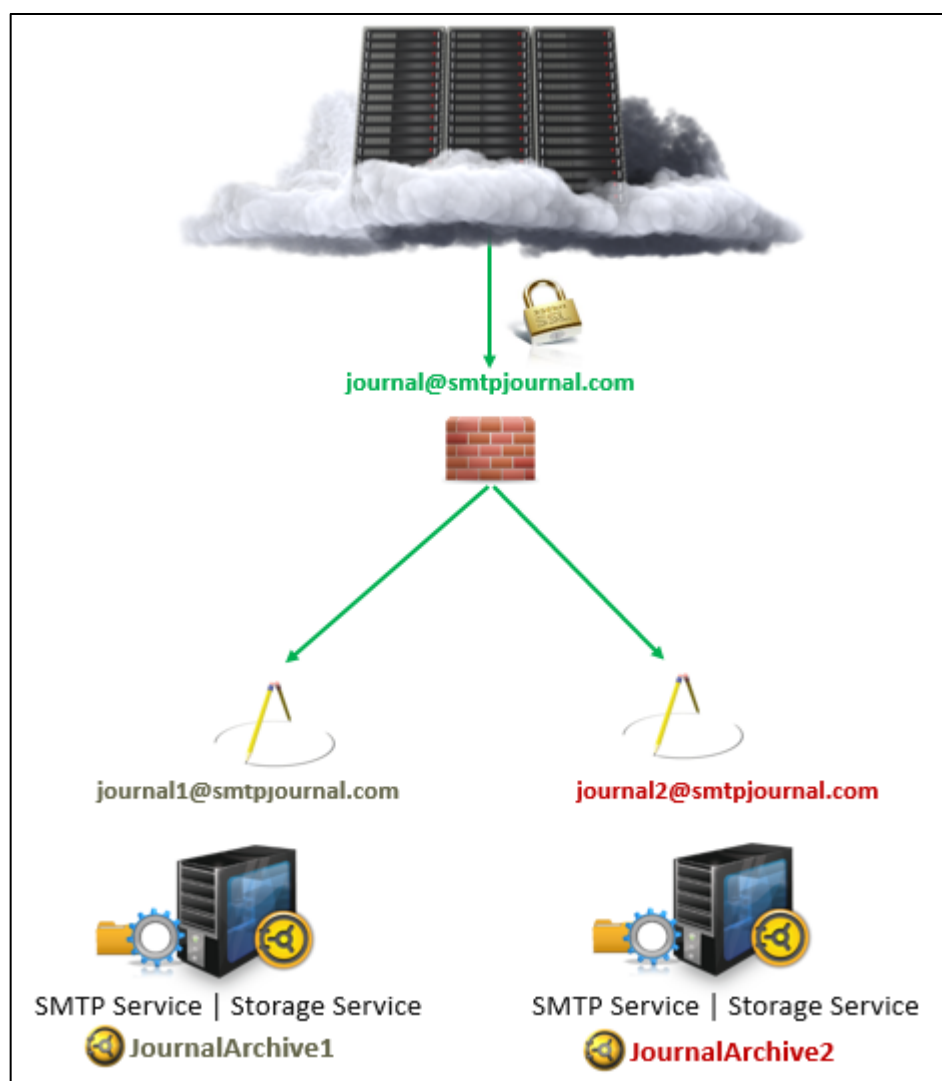


Figure 8 – SMTP Archiving for Cloud Messaging Platforms

In this scenario address rewriting is used to distribute the journal email across two Enterprise Vault servers. The load balancing is done by the firewall (using MX records) but can also be done with a hardware load balancer.

To configure mail routing from the cloud provider to your on-premise Enterprise Vault server, an externally resolvable domain name is required, for example mycompanyjournaldomain.com. A certificate will also be required to encrypt the journal emails.

Configure the Enterprise Vault environment (See Appendix Band Appendix C), and configure the firewall and/or load balancer to deliver email on secure SMTP to the Enterprise Vault servers.

Configure Journaling for Office 365

To configure this connector in Office 365, log in to the Exchange Admin Center. Click on Compliance Management, then Journal Rules. Create a new journal rule as per Figure 9.

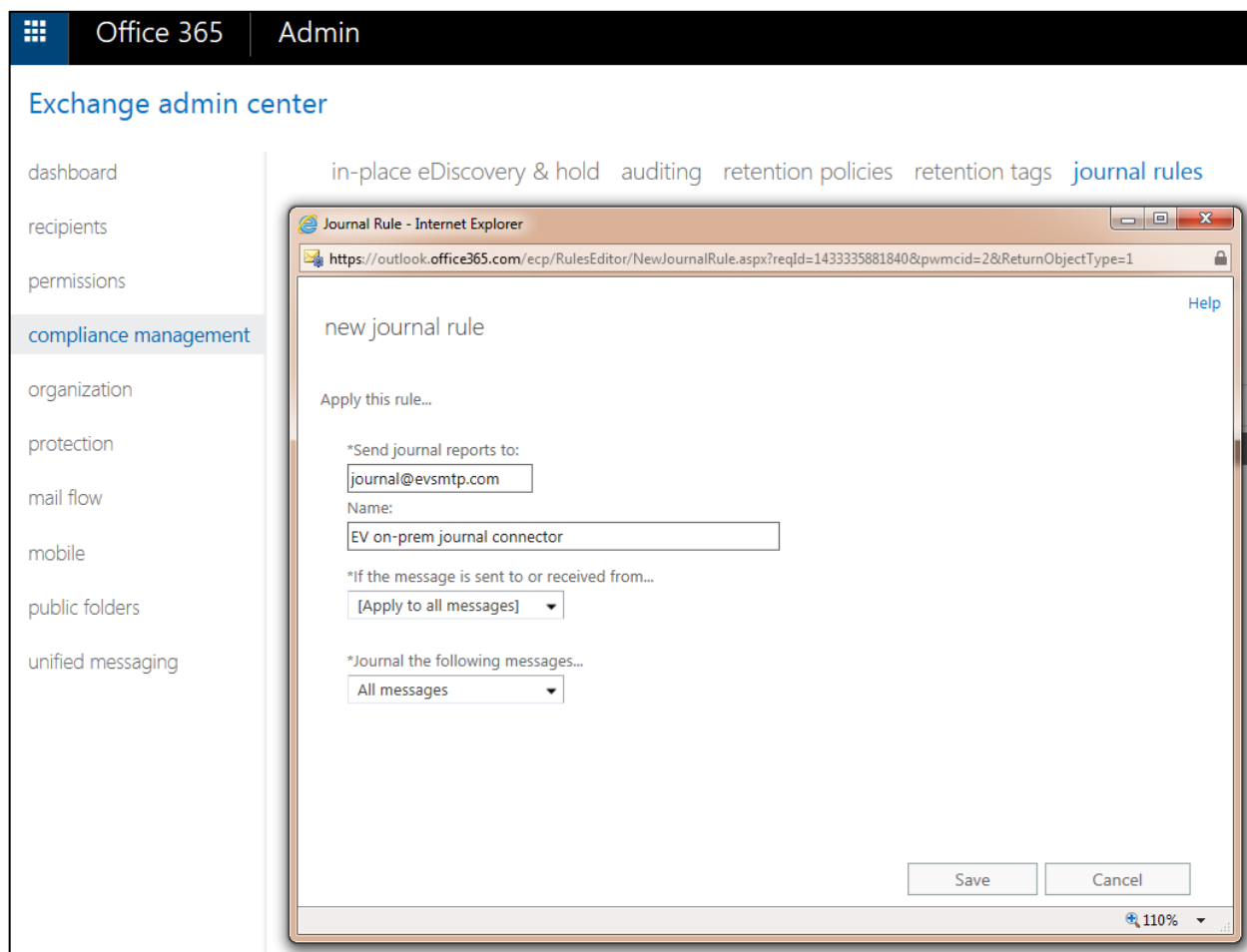


Figure 9 – Office 365 Journal Rule

The rule will not become active until an existing Office 365 email account is configured to receive undeliverable emails for the Office 365 organization. The mailbox you select to receive the undeliverable emails can be helpful if troubleshooting is required.

Refer to article “Setting up Exchange Server and Office 365 for Enterprise Vault SMTP Archiving” available at https://www.veritas.com/support/en_US/article.000116527.

Native Decryption for Office365

From Enterprise Vault 12.4 and later, native decryption is supported for Office365 emails through Azure RMS service. Native decryption will help for storage optimization, preview and search RMS protected items through Enterprise Vault Search and Accelerator add-on products. Customers can also export items in decrypted format using the EmlDecryptor utility.

Configure Journaling for Gmail

Similar to Office 365 ensure the externally resolvable domain is configured, the Enterprise Vault environment set up and the firewall is configured to accept and forward the secure SMTP traffic to the Enterprise Vault servers.

Log in to the Google Apps Administration console, and navigate to the Gmail Advanced settings.

Click on Add Setting.

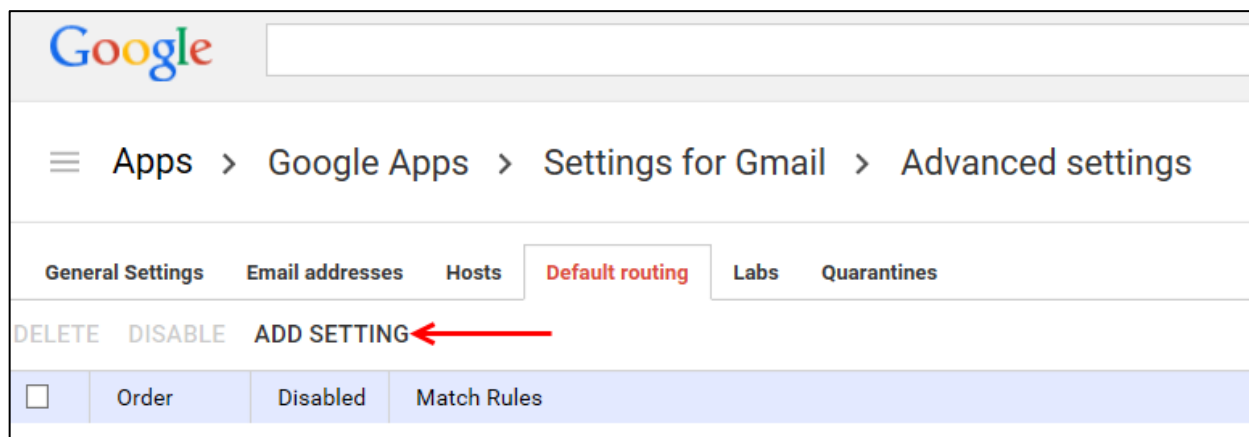


Figure 10 – Gmail Advanced Settings

Choose the required level of journaling (All Recipients in this example).

Add setting

1. Specify envelope recipients to match

Single recipient ▼

- Single recipient
- Pattern match
- Group membership
- All recipients

2. If the envelope recipient matches the above, do the following

Modify message ▼

Headers

- ☐ Add X-Gm-Original-To header
- ☐ Add X-Gm-Spam and X-Gm-Phishy headers
- ☐ Add custom headers

Subject

- ☐ Prepend custom subject

Route

- ☐ Change route

Envelope recipient

- ☐ Change envelope recipient

Save Cancel

Figure 11 – Gmail Journal Console (1/2)

Scroll down and select “Add more recipients”. Enter the recipient address, and select the “Perform this action on non-recognized and recognized addresses”. Click Save to complete the configuration.

Add setting

Attachments

☐ Remove attachments from message

Also deliver to

☒ Add more recipients

Recipients

ADD

Basic

Recipient address:
evjournal@mysmtpjournaldomain.com

CANCEL SAVE

3. Options

☐ Perform this action only on non-recognized addresses

☒ Perform this action on non-recognized and recognized addresses

Save

Cancel

Figure 12 – Gmail Journal Console (2/2)

PowerShell

The following PowerShell commands are available to use with SMTP Archiving. The commands can be run from the Enterprise Vault Management Shell interface.

PowerShell cmdlet	Description
Get-EVSMTPPolicy	Retrieves the properties of an existing SMTP Policy
New-EVSMTPPolicy	Creates a new SMTP policy
Set-EVSMTPPolicy	Updates the properties of an existing SMTP policy
Remove-EVSMTPPolicy	Deletes an SMTP policy
Get-EVSMTPTarget	Retrieves the properties of an existing SMTP target
New-EVSMTPTarget	Adds a new SMTP target address
Set-EVSMTPTarget	Updates the properties of an existing SMTP target address
Remove-EVSMTPTarget	Deletes an SMTP target address
Get-EVSMTPServerSettings	Retrieves the SMTP server settings for all the Enterprise Vault SMTP servers in the site
New-EVSMTPServerSettings	Creates the SMTP server settings for all Enterprise Vault SMTP servers in the site
Set-EVSMTPServerSettings	Updates the SMTP server settings for all Enterprise Vault SMTP servers in the site
Sync-EVSMTPServerSettings	Synchronizes the SMTP server settings in the directory with the settings on an Enterprise Vault SMTP server
Get-EVSMTPHoldingFolder	Retrieves details of the SMTP holding folder that is configured for the SMTP Archiving task on the current Enterprise Vault server

For information on how to manage X-Header lists, type: `get-help about_SMTPXHeaders`.

The following commands provide information on managing the authentication of incoming connections to the SMTP servers:

- `get-help about_SMTPConnectionControlList`
- `get-help about_SMTPEnumerations`
- `get-help about_TlsCertificate`

X-Headers

X-Headers are additional properties added to an SMTP message by the originating application or a routing SMTP server.

Some applications provide built-in capability to add X-headers to a message - Exchange 2013 for example can use transport rules to add content. Other applications use routing MTAs (message hygiene applications for example) to add x-headers to emails, such as spam reputation scores.

Enterprise Vault SMTP Archiving can handle X-headers in two different ways:

- Index information held in X-headers so it can be displayed and searched in applications like Discovery Accelerator
- Act on specific “x-KVS-” X-headers to archive to a specific Archive, or use a different Retention Category.

The following table shows the X-Headers that can be used by Enterprise Vault.

X-Header	Description
X-Kvs-ArchiveId	<p>This header can be used to identify a different archive from the one that is configured for the target address in the message</p> <p>Example: X-KvsArchiveId:160EEB784C7DFEE1210000evserver1</p>
X-Kvs-RetentionCategory	<p>Provides the ID of the retention category to assign to the message, different from the category configured for the target address.</p> <p>Example: X-Kvs-RetentionCategory:1505EB5F98000evserver1</p>
X-Kvs-OriginalLocation	<p>Overrides destination folder in the archive, by default items will be archived to the “Inbox” folder but by using x-kvs-OriginalLocation, the folder can be changed to something else.</p> <p>Example: X-Kvs-OriginalLocation:CompanyA\ProductB</p>
X-Kvs-MessageType	<p>Identifies the type of the message. For example: Bloomberg,IM.</p> <p>This header is used to override the value of the Vault.MsgType property that is assigned to the message when it is archived. By default, the SMTP archiving task assigns the value SMTP.mail to the Vault.MsgType property</p>
X-Kvs-IndexData	<p>Used to provide one or more properties for Enterprise Vault to index.</p> <p>Using standard X-Headers, you can only add one property per X-Header. The X-Kvs-IndexData header allows you to add several properties in the one X-Header. The header contents are specified using XML.</p>

After adding new X-Header fields the SMTP Archiving Task on each Enterprise Vault server needs to be restarted.

Using X-Headers with Enterprise Vault Search

Enterprise Vault Search can be configured to display additional x-headers that have been indexed. To do this, right-click on the columns bar and select customize columns.

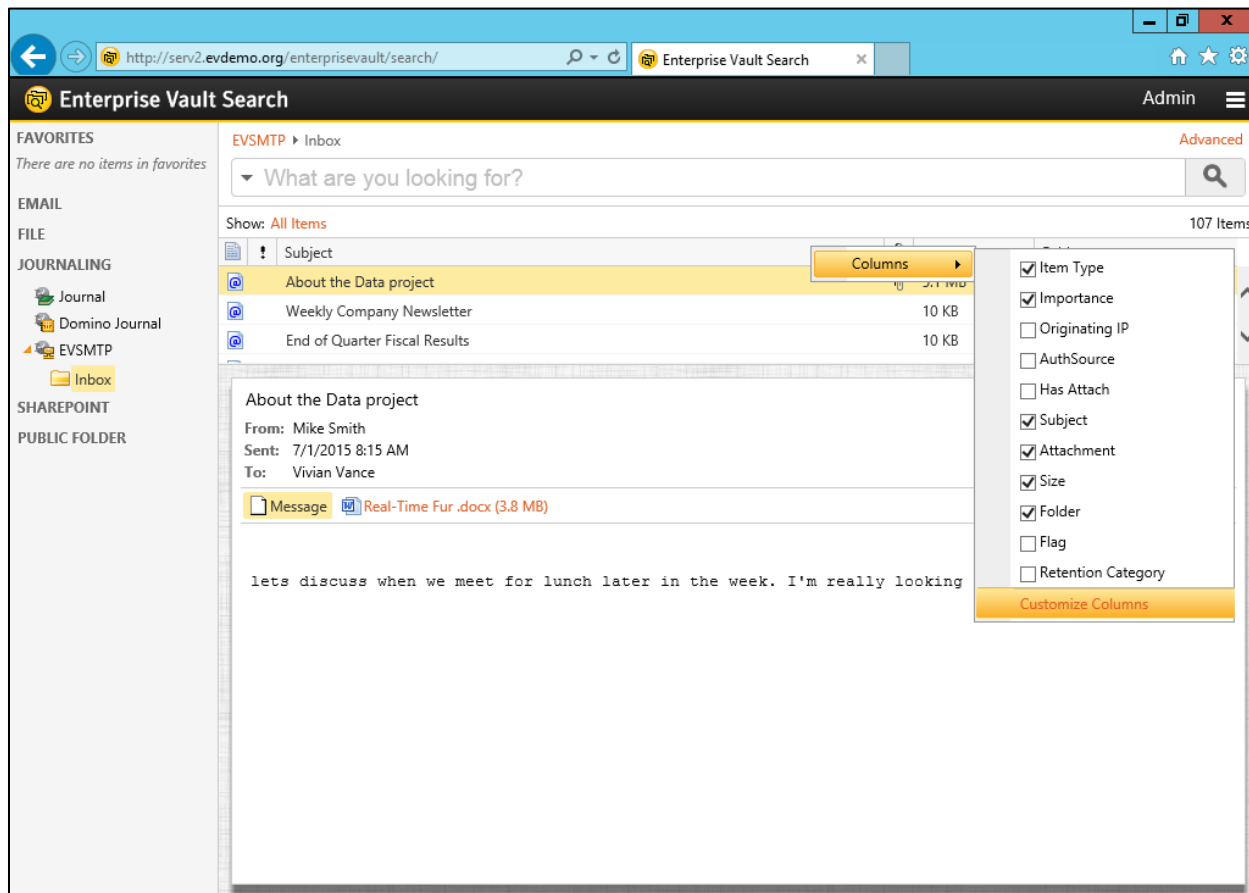


Figure 13 – Configuring EVS to show X-Headers

To show the x-header values in the search results screen, type in `EVXHDR.thenameofyourxheader`. Under Column Header, and the column header name.



Customize Columns

Choose the columns you want to see and change their order within the results pane. You can use only white text boxes to modify and add item properties.

Property Name	Column Header	Order
<input type="checkbox"/> msgc	Item Type	
<input type="checkbox"/> impo	Importance	
<input checked="" type="checkbox"/> EVXHDR.X-Originating-IP	Originating IP	
<input checked="" type="checkbox"/> EVXHDR.X-MS-Exchange	AuthSource	
<input checked="" type="checkbox"/> EVXHDR.X-MS-Has-Attach	Has Attach	
<input checked="" type="checkbox"/> subj	Subject	
<input type="checkbox"/> natc	Attachment	
<input type="checkbox"/> size	Size	
<input type="checkbox"/> clif	Folder	
<input type="checkbox"/> flag	Flag	
<input type="checkbox"/> crcn	Retention Category	

Help Reset Done

Figure 14 – Configuring EVS to show X-Headers

The X-Headers will now be displayed in the appropriate columns (Figure 16).

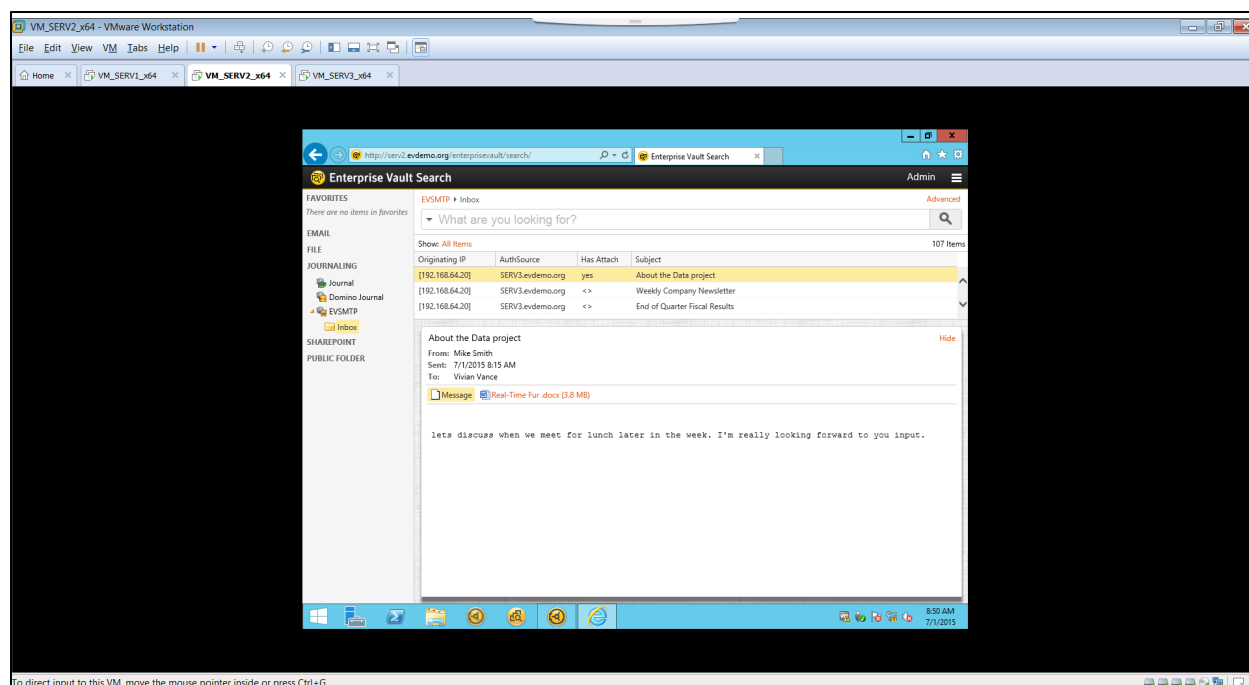


Figure 15 –X-Headers fields showing in EVS

Using X-Headers with Discovery Accelerator

With the Discovery Accelerator Search interface there is a free form attribute field where you can add indexed x-headers to search against (Figure 17).

Free form attribute	Attribute: EVHXDR.X-Origin	Type: String	Operator: Any	Value: 192.168.64.20
Free form attribute	Attribute:	Type: String	Operator: Any	Value:

Figure 16 –Free form attribute in Discovery Accelerator

If you regularly search against certain x-headers within Discovery Accelerator, you can also easily configure the search interface so that the x-header is a built-in option. To do this, add a search attribute (Figure 18).

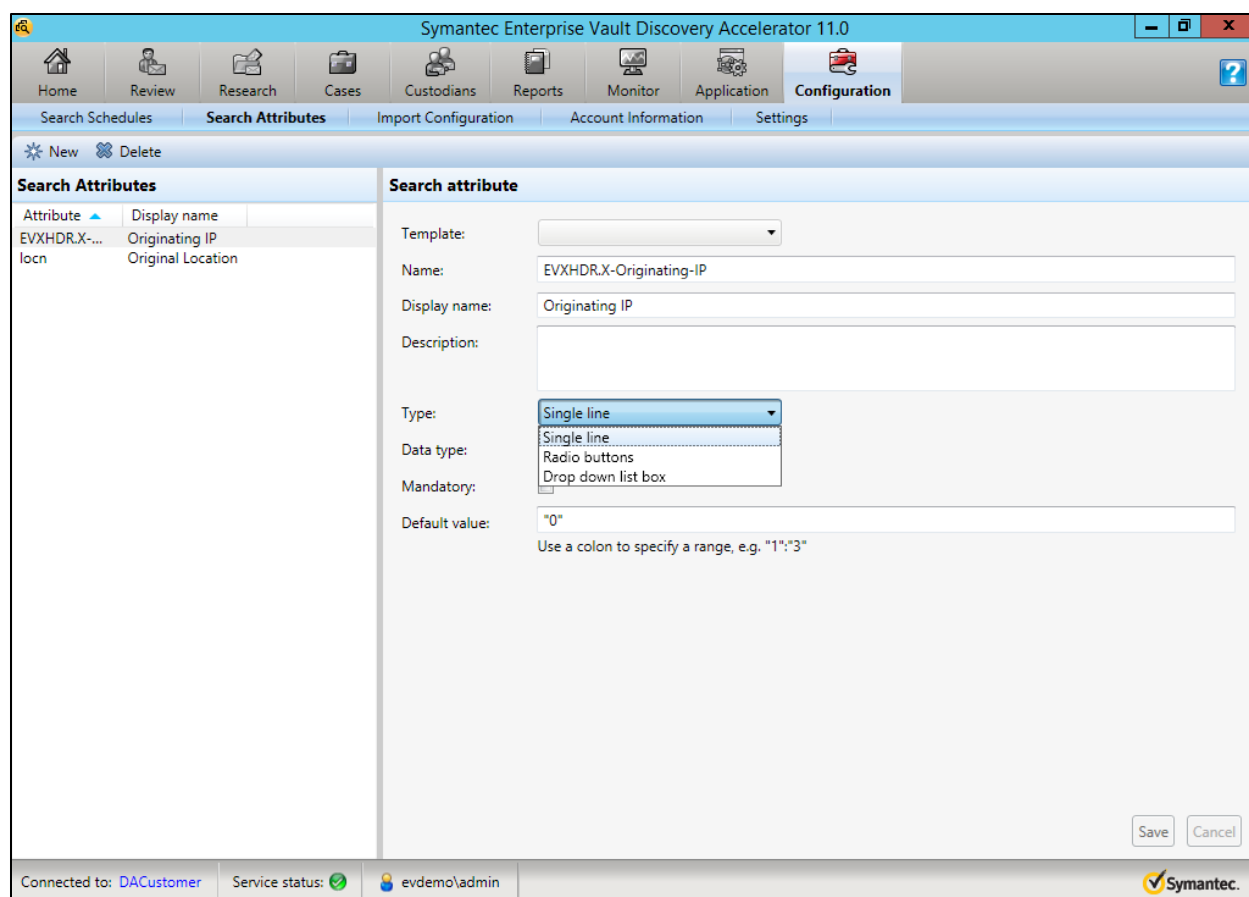


Figure 17 –Adding Search Attributes in Discovery Accelerator (1 of 2)

Within Discovery Accelerator, select Configuration/Search Attributes, and click New. Type in the name of the X-header, and the Display Name. Choose how you would like the search values to appear. In the form of a single line, radio buttons or a drop down list.

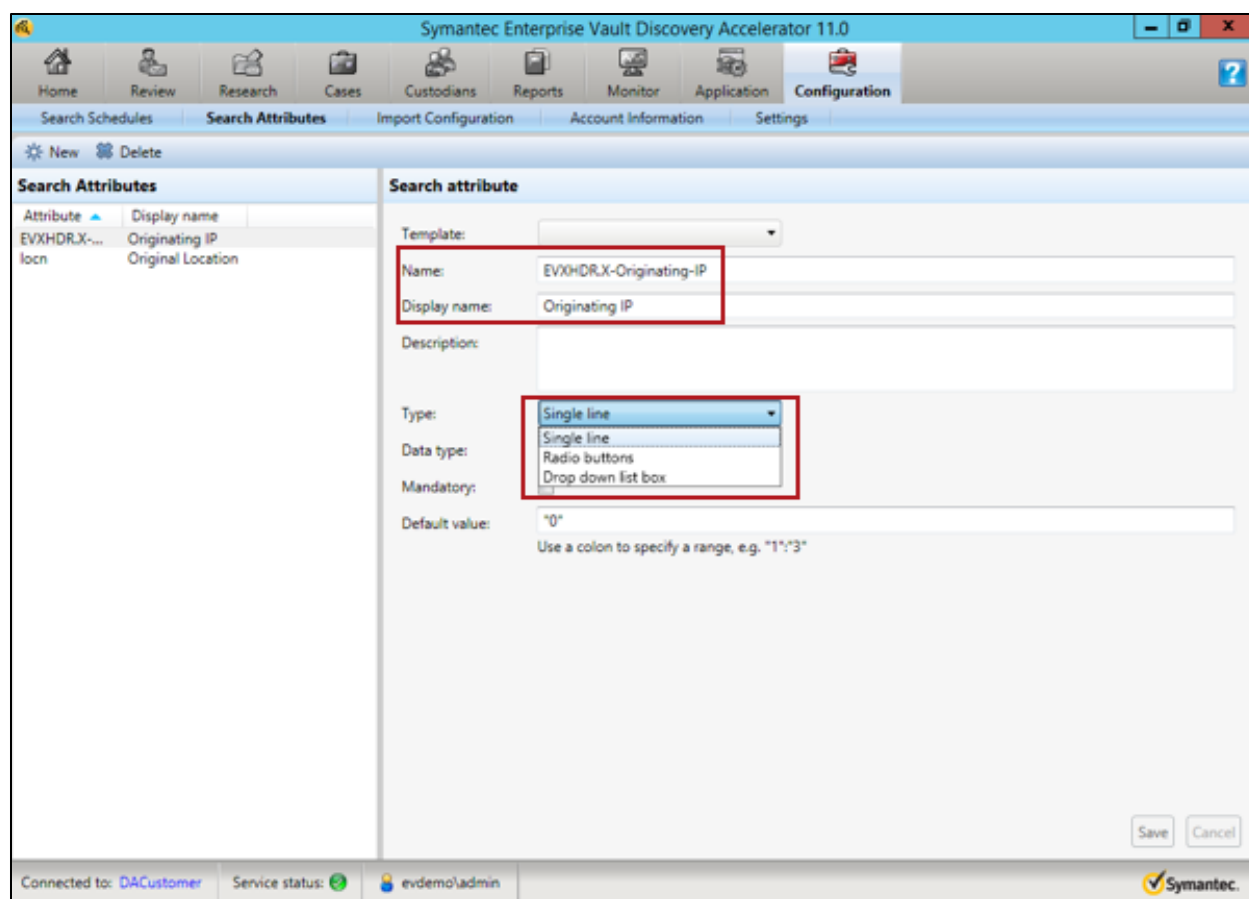


Figure 18 –Adding Search Attributes in Discovery Accelerator (2 of 2)

Now add the Data type for the X-header - whether it is in the format of a string, number, or date, and click Save.

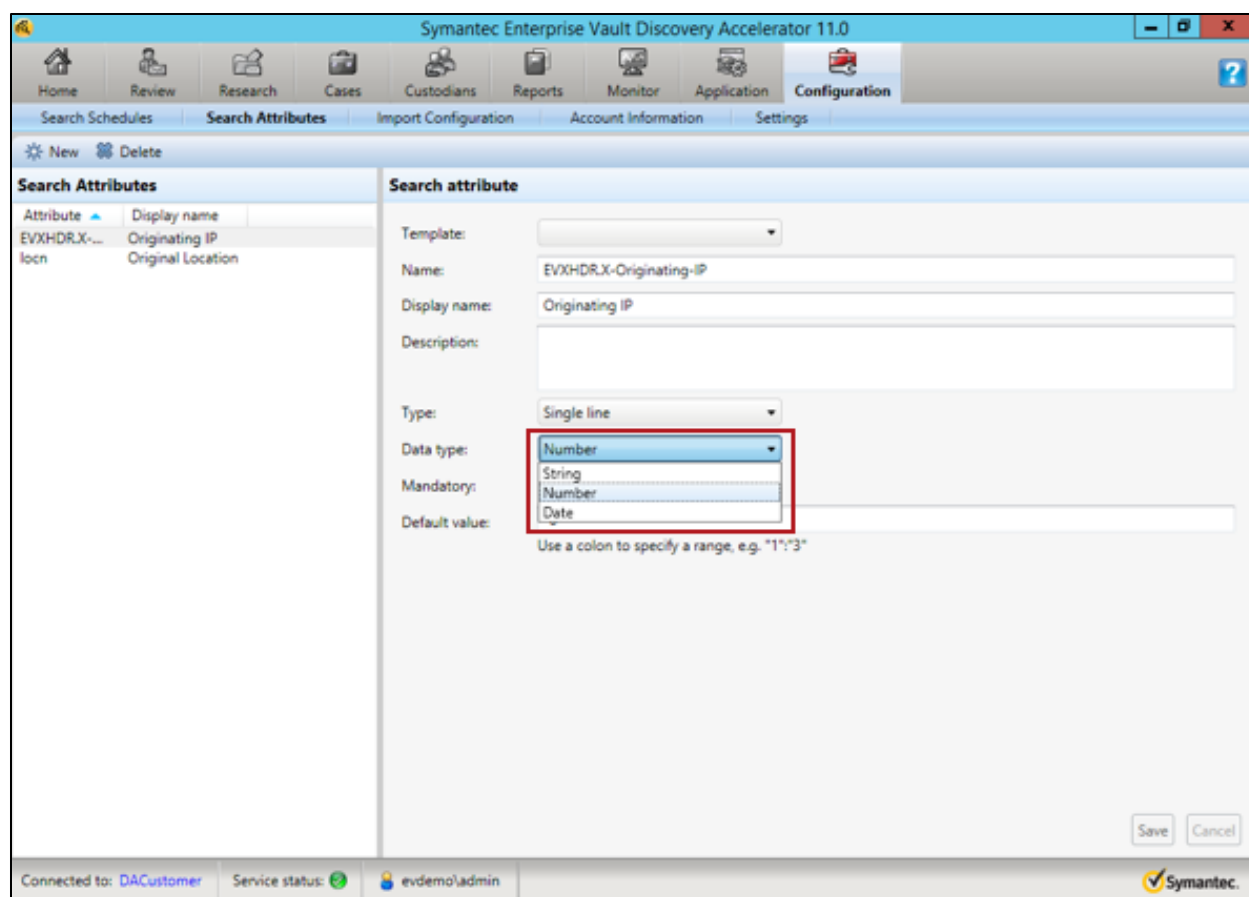


Figure 19 – Adding Search Attributes in Discovery Accelerator

In the above example we now have a new field to search against within our Discovery Accelerator search interface, called Originating IP. Click Save to run the search.

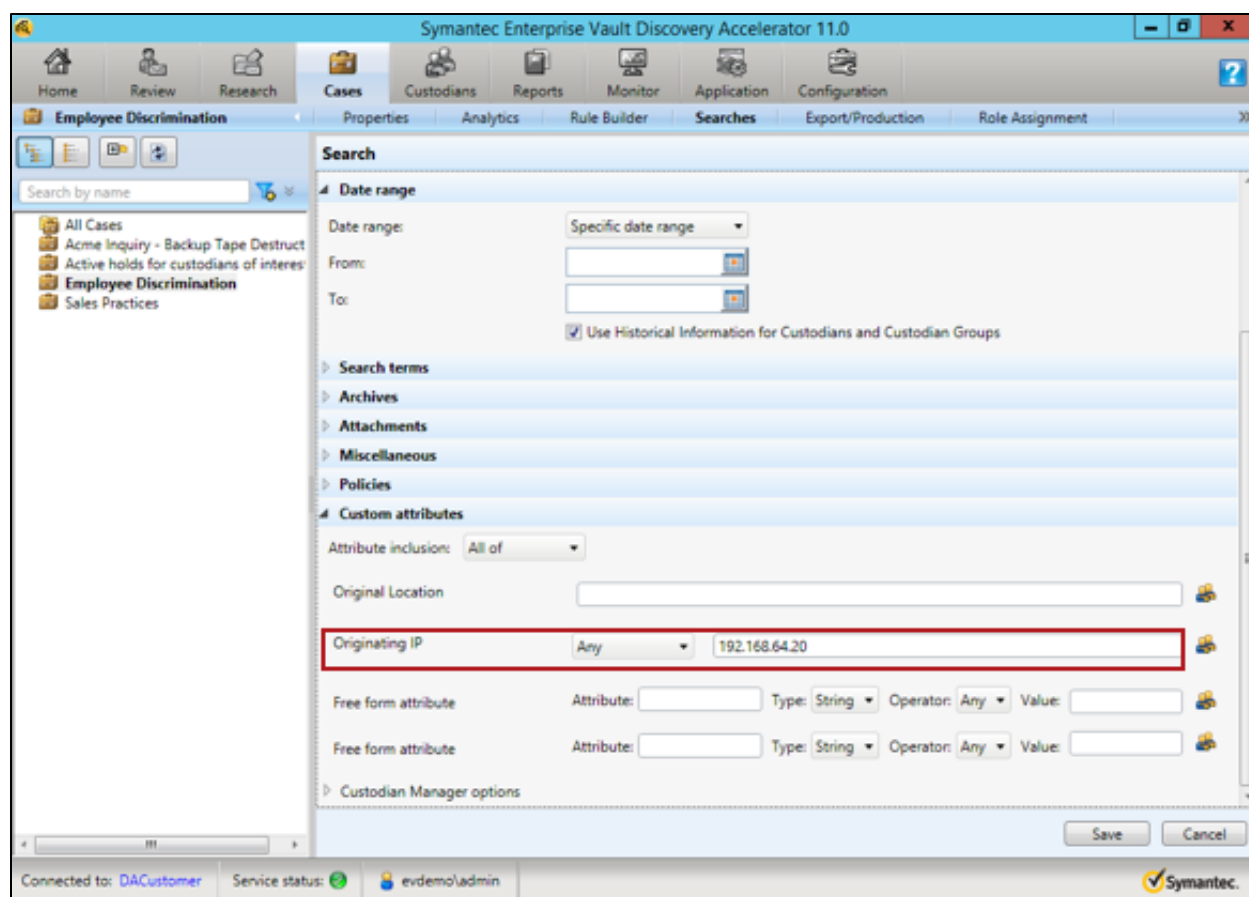


Figure 20 – Adding Search Attributes in Discovery Accelerator

The test search returns four hits, with the X-header field highlighted.

Within Discovery Accelerator, you can select the search you performed on the x-header and it returns all emails with the originating IP Address that was searched upon.

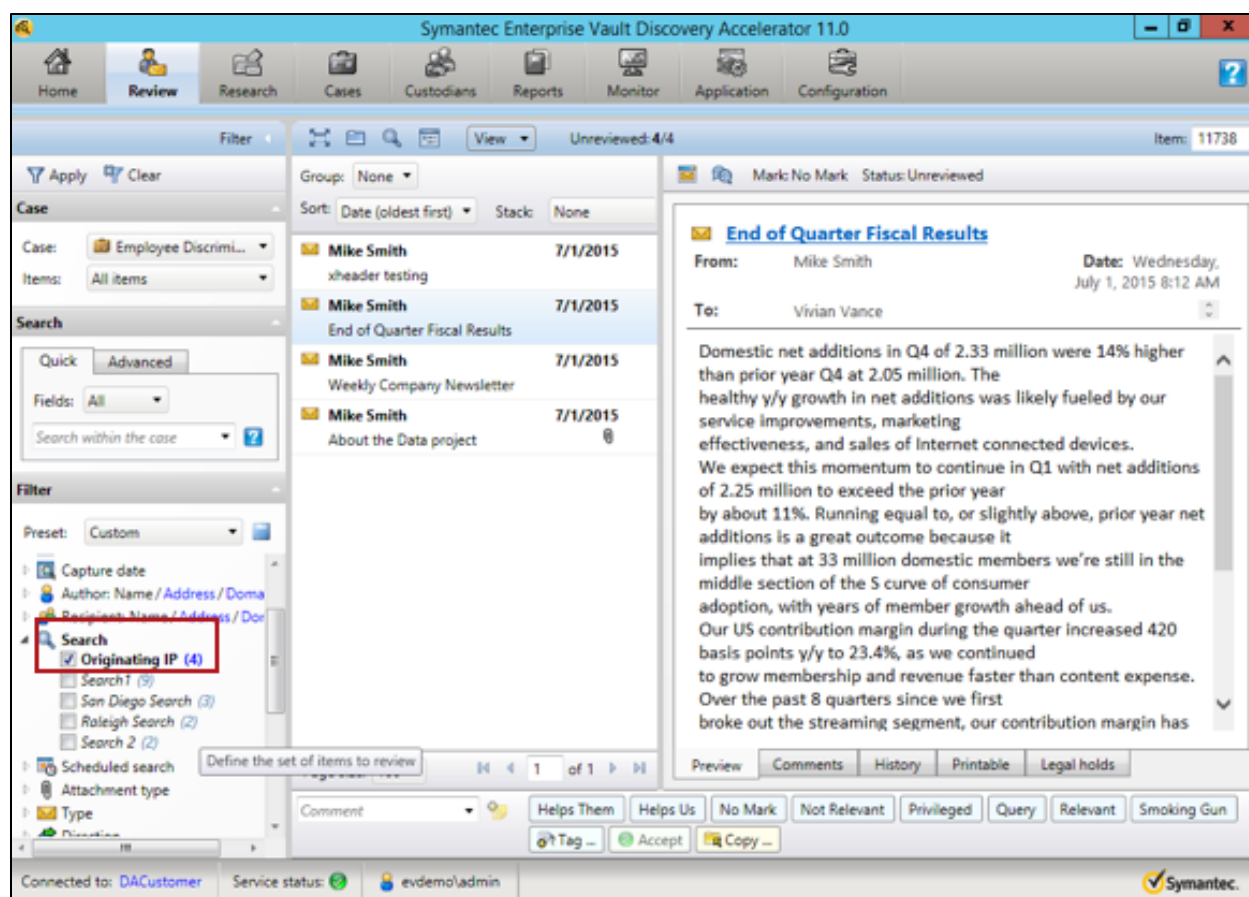


Figure 21 – Adding Search Attributes in Discovery Accelerator

If we open up one of the messages we searched on, the x-header appears with the appropriate value.

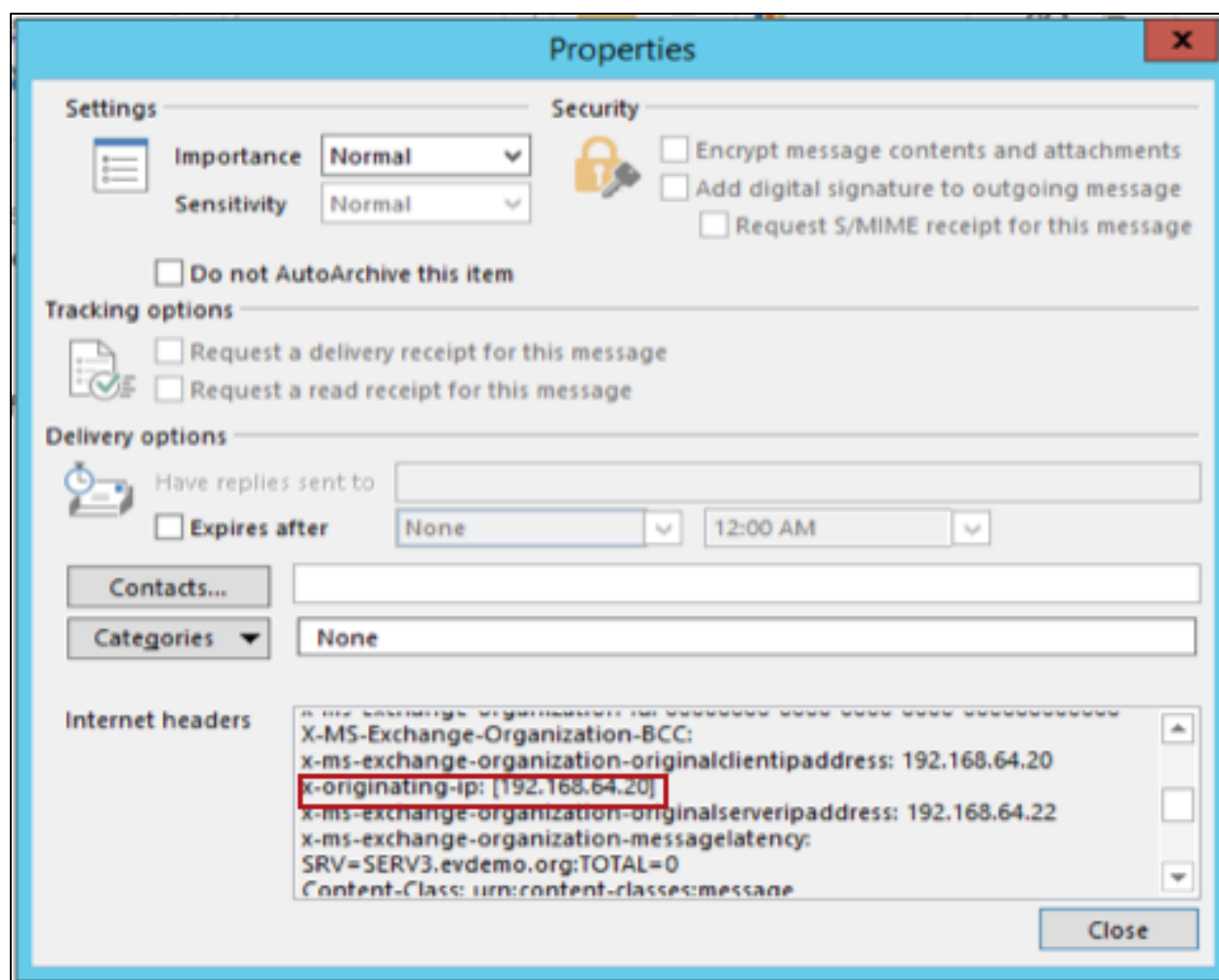


Figure 22 – Adding Search Attributes in Discovery Accelerator

For more configuration details see referenced document “Setting Up SMTP Archiving.pdf”.

Monitoring and Reporting

The standard monitoring and reporting features within Enterprise Vault have been updated to include SMTP Archiving.

Figure 23 shows the SMTP Archiving Task Summary, found in the Reports directory.

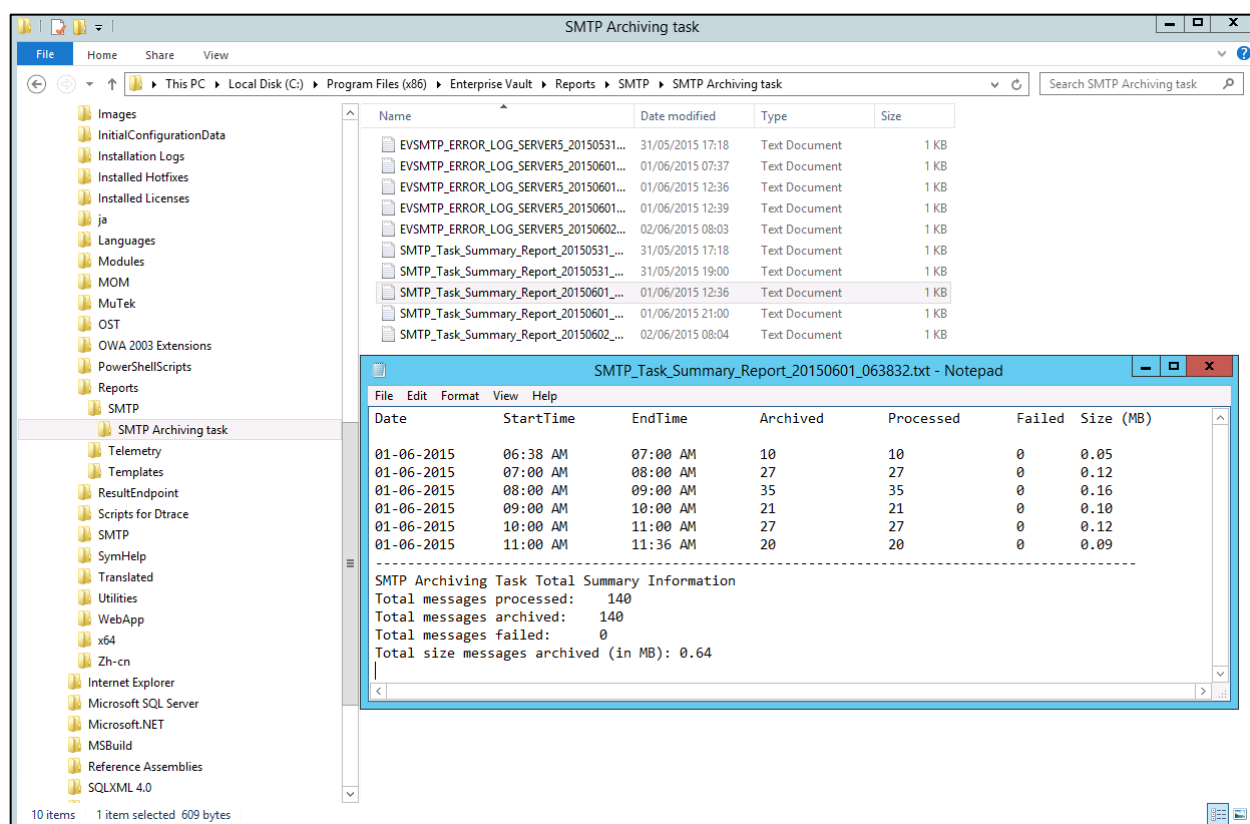


Figure 23 – SMTP Task Summary

Enterprise Vault ships with a SCOM Pack that will allow the administrator to easily monitor the solution. The SCOM pack is designed to:

- Provide information on the performance and health of SMTP Archiving task and SMTP Server.
- Notify the administrator of unexpected inflow, archiving and failure rate.
- Notify administrator of events so that he can take corrective action, for example:
 - Certificate Expiry
 - Holding folder capacity reaching 90%
 - SMTP Archiving task has stopped

The following are default alert settings, and should be adjusted following the implementation:

- Number of mails archived goes below 1,000 emails per day.
- Number of mails archived goes above 100,000 emails per day.
- Number of mails failed to archive goes above 100 emails per day.
- Number of mails received by SMTP Server goes below 1,000 emails per day.
- Number of mails received by SMTP Server goes above 100,000 emails per day.
- Number of mails for which failure was reported goes above 10 emails per day.

All the above alerts are visible in Event log, System Status and SCOM.

The following Windows Performance Counters can be monitored by any 3rd Party monitoring application:

- SMTP Performance counters:

Performance Counter	Description
Maximum original size of SMTP messages (bytes)	Shows size of biggest messages archived so far
SMTP messages archived	Shows total number of messages archived by SMTP archiving task
SMTP messages original size(bytes)	Shows total size of messages archived so far in bytes
SMTP messages processed	Shows total number of messages processed by SMTP archiving task
SMTP messages unable to archive	Failure to archive the message, for example when the storage service is not available.

Table 5 - SMTP Performance Counters

- SMTP Holding Folder performance counters:

Performance Counter	Description
Connectivity	Connectivity is 1 if the Holding folder accessible
Disk Space % used	Shows percentage used space on the disk where the holding folder resides

Table 6 – Holding Folder Performance Counters

- SMTP Service Performance counters:

Performance Counter	Description
Concurrent connections	Shows number of concurrent connections made from various SMTP clients to EV SMTP service at that instance of time
Connection rejected	Shows total number of connections rejected by Enterprise Vault SMTP server. Connections can be rejection due to various reasons, for example, a connection control list is specified and the client machine is not in the connection control list
SMTP message original size (bytes)	Shows total size of messages received so far in bytes
SMTP messages received	Shows total number of messages received by Enterprise Vault SMTP service
SMTP messages rejected	Shows total number of messages rejected by Enterprise Vault SMTP service. Mail can get rejected if the max message size is set on Enterprise Vault server and client is sending mail which is bigger than the specified size

Table 7 – SMTP Service Performance Counters

Troubleshooting

Dtrace is an Enterprise Vault utility that can be used to see low-level tracing information on particular processes, and can be helpful in troubleshooting. To find out more information about the utility refer to the Utilities.pdf file in the product media.

To assist with troubleshooting SMTP, enable Dtrace for the following:

- SMTP archiving task: Set EvSMTPTask verbose **yes**
- SMTP service: Set isode.pp.smtp verbose **yes**

Alternatively traces can also be configured the Vault Administration Console.

Table 8 details further troubleshooting considerations.

Issue	Troubleshooting Steps
Enterprise Vault SMTP service fails to start	<ul style="list-style-type: none"> • Verify Enterprise Vault SMTP service port is not being used by any other application • If the port is in use change it
SMTP service settings are not getting applied on any Enterprise Vault server	<ul style="list-style-type: none"> • Check the network connectivity • If Enterprise Vault server is accessible, restart Enterprise Vault Admin service to sync SMTP server settings
Mails are not received in the Holding folder	<ul style="list-style-type: none"> • Verify the target email address is configured correctly • Verify the holding folder is configured and accessible • Verify if connection rejection counter or mail rejection counter is incremented • Verify the Enterprise Vault SMTP server settings • Check Event Viewer
Mails are being received but not getting archived even if targets and SMTP server setting are configured correctly	<ul style="list-style-type: none"> • Restart the EV SMTP Archiving Task • Check for EVSMTP_ERROR_LOG files which are in EVInstallDir\Reports\SMTP\SMTP Archiving task name

**SMTP Archiving task is not in
“Processing” state**

- Check if task controller service is up and running

Table 8 – Troubleshooting issues

Licensing Considerations

A valid license for Exchange or Domino Journaling will entitle customers to SMTP archiving. New customers receive SMTP Journaling as part of the eDiscovery bundles. For SMTP Mailbox Journaling the Email Management license is required.

Appendix A Frequently Asked Questions

Q: How can I setup Exchange, Office 365 or Domino journaling to specific SMTP address?

A: There are two ways to setup Exchange to send a journal copy of messages to a SMTP address

- **Standard journaling:** Standard journaling is configured on a mailbox database. It enables the Journaling agent to journal all messages sent to and from mailboxes located on a specific mailbox database.
- **Premium journaling:** Premium journaling enables the Journaling agent to perform more granular journaling by using journal rules. You must have an Exchange Enterprise client access license (CAL) to use premium journaling.

Q: With new Enterprise Vault SMTP Archiving in Enterprise Vault 11.0.1, will the existing Exchange or Domino journaling functionality, via journal mailbox, be removed?

A: No. The existing Exchange and Domino agent will be available.

Q: Will the new Enterprise Vault SMTP Archiving work seamlessly with Discovery Accelerator and Compliance Accelerator?

A: Yes. Enterprise Vault 11.0.1 also includes enhancements to Discovery Accelerator and Compliance Accelerator, providing support for supervision and discovery of information ingested via the new SMTP Agent.

Q: What will happen in the event of loss of connectivity between Exchange Server and Enterprise Vault SMTP server(s)?

A: It is recommended that the Enterprise Vault SMTP service be deployed on multiple servers. If required, make the Enterprise Vault SMTP servers highly available to avoid loss of connectivity. In the event of total loss of connectivity between the Exchange MTA forwarding the journal feed and the Enterprise Vault SMTP server(s), the emails will be queued on the Exchange MTA server depending on the queue size and available storage.

Q: Does SMTP Archiving support message Single Instance Storage?

A: Yes.

Q: Can Exchange be configured to journal emails to a journal mailbox and also send a copy to a SMTP address hosted by Enterprise Vault SMTP server?

A: Yes. This can be configured via multiple journal rules, one sending a copy to journal mailbox, and the other sending a copy to the SMTP address hosted by Enterprise Vault SMTP server.

Q: Will Enterprise Vault SMTP Archiving work with AD-RMS protected emails?

A: If journal report decryption is configured on Exchange Server 2013 or Exchange Server 2010, then two messages are attached to the journal report: the original RMS-protected message and a clear text version. A policy setting controls whether Enterprise Vault uses the clear text message or the RMS-protected message as the primary message during archiving.

Q: How can I monitor queue size(s) for SMTP?

A: The Enterprise Vault SCOM pack supports monitoring of various different parameters related to SMTP archiving agent such as task, service and holding folder. Performance counter for SMTP service monitor the number of messages received, number of messages rejected etc.

Appendix B Deployment Prerequisites

The deployment prerequisites for Enterprise Vault 11.0.1 are the same as Enterprise Vault 11.0.0. The Enterprise Vault Compatibility Charts (<http://www.symantec.com/docs/TECH38537>) contains details of the supported versions of prerequisite software.

The default port used by SMTP on Enterprise Vault SMTP Server is 25, which can be changed using the SMTP Server Configuration settings to accommodate specific firewall or security requirements.

The SMTP archiving component is enabled on a per server basis when performing the upgrade to Enterprise Vault 11.0.1, or can be added later by running Setup.exe from the installation media.

Once installed, the “Enterprise Vault SMTP Service” will be listed under the Windows Services Management console on the server.

Appendix C Configuring SMTP Journaling for Exchange Server

This section will detail configuration for the following scenario:

The customer wishes to enable Journaling for all 50,000 users in their environment. Initially the pilot solution will only involve 5,000 users on a single Exchange 2013 server.

The customer does have a Microsoft Enterprise Client Access license and is therefore entitled to use the Premium Journaling option in Exchange. During the pilot the administrator will use the database level journaling to only enable a number of users on a particular database, and following the successful pilot the intention is to use transport level journaling to enable all users.

Configure Exchange Contact

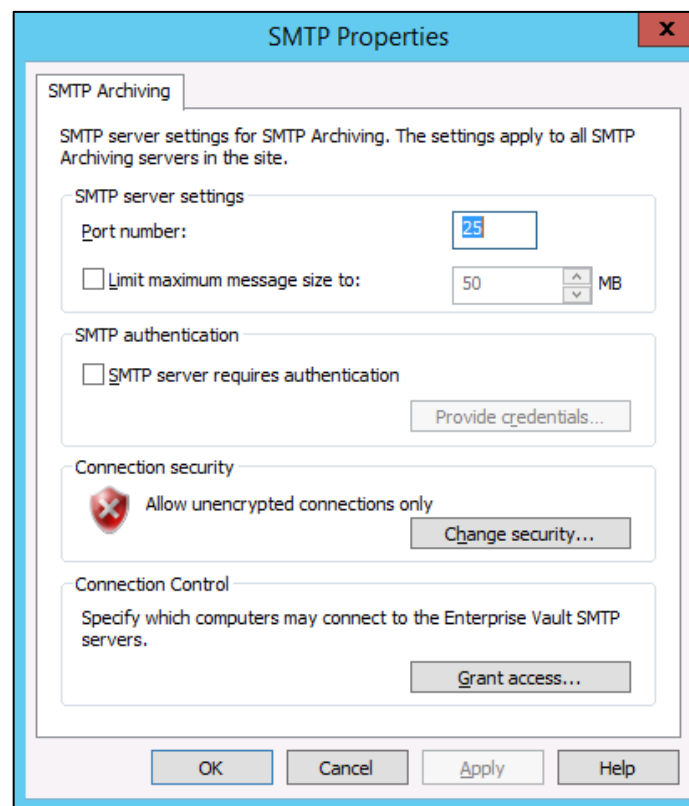
This is an optional step, and only required for earlier versions of Exchange Server where the journal recipient address must exist as a Contact.

Create the Exchange Send Connector

Refer to Appendix D and Appendix E.

Configure the EV SMTP service.

Access the SMTP Service Configuration by right-clicking and choosing Properties on the SMTP node, under Targets. Configure the SMTP port number (if required), and configure any connection control or encryption properties.

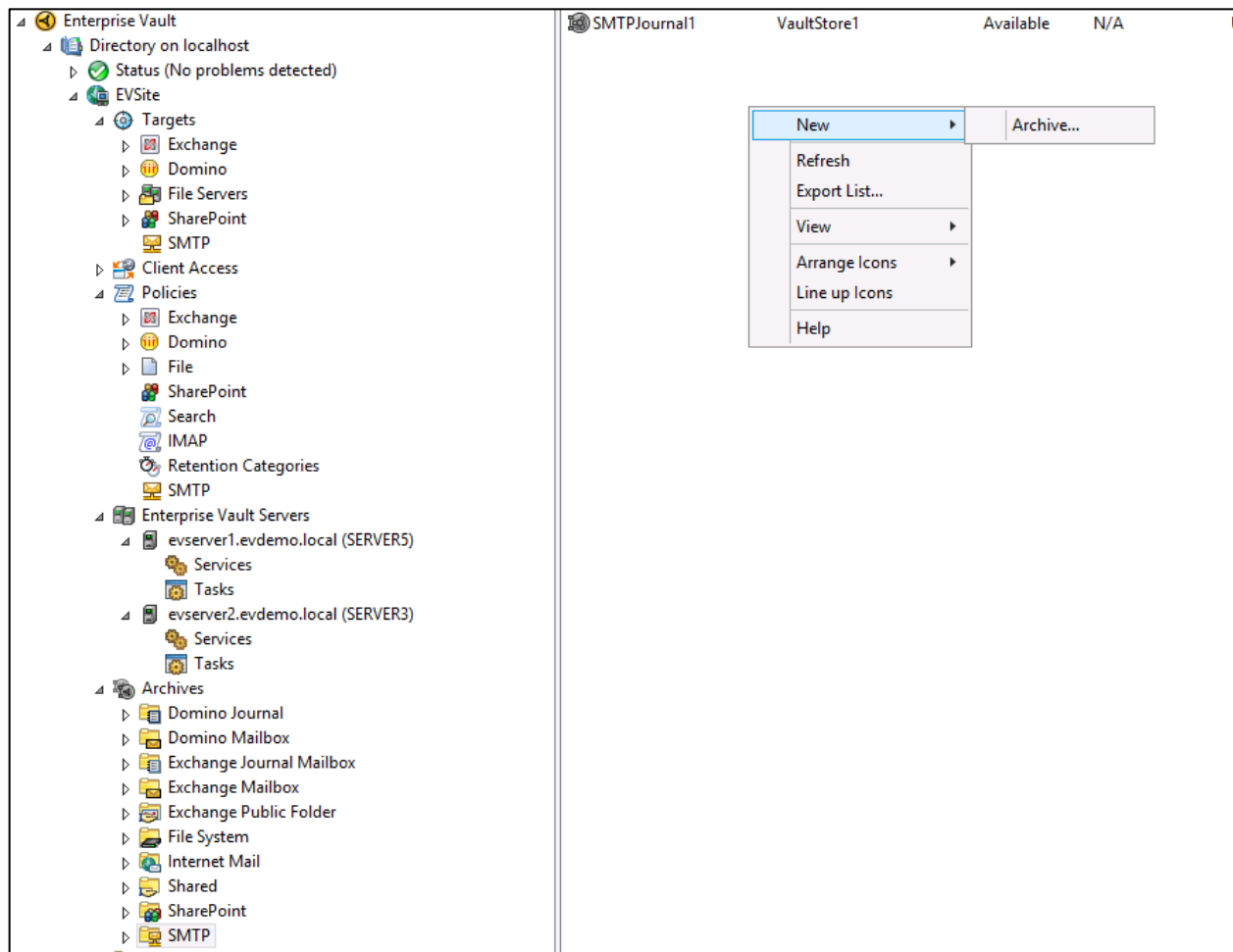


Create the EV SMTP Archives.

Any Journal archive type can be used, it doesn't have to be an SMTP archive. Importantly it should not be metadata enabled archives for SMTP Journal email, as the archive will grow the Vault Store database at a faster rate. Metadata enabled archives are only required if the archives are to be accessed by end users – they provide faster Enterprise Vault Search listing of items.

In order to make use of both storage services, ensure the archives are created in the Vault Store associated with the local storage service. In other words create SMTPJournal1 in VaultStore1 (hosted by the Storage Service on the EVSMTP1 server), and SMTPJournal2 is in VaultStore2 (hosted by the Storage Service on the EVSMTP2 server).

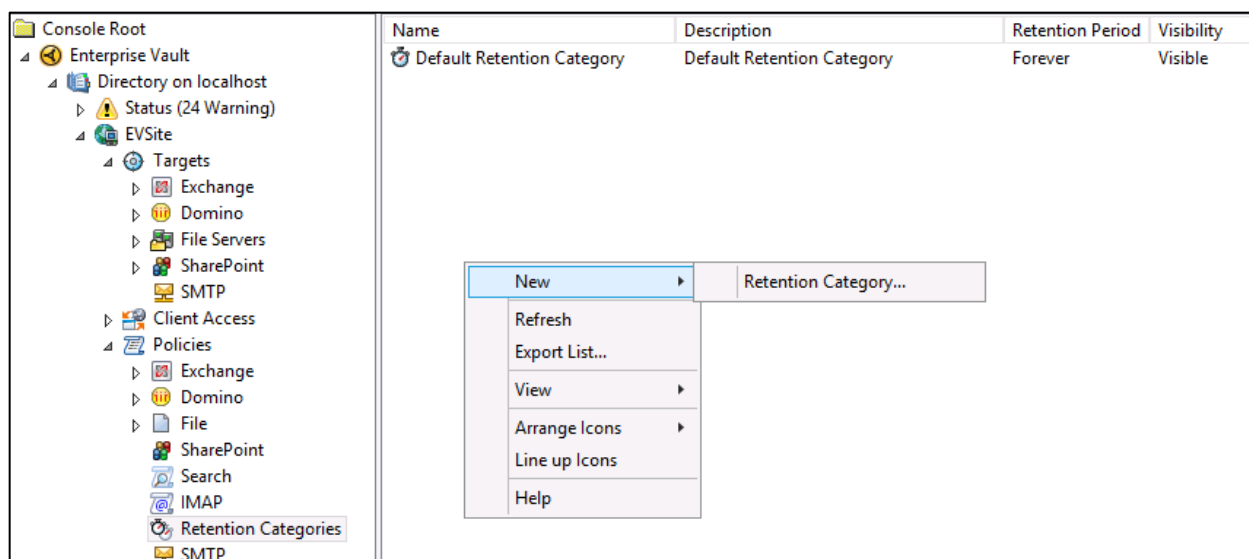
To create the archives, right-click on the SMTP container in Archives, and choose New.



Close the wizard after creating both archives.

Configure the Retention Category for SMTP Journaling

It is recommended that a new Retention Category is created specifically for SMTP Journaling. If you require more than one retention category create it now.



Click Next. Enter an appropriate name and description for the retention category.

The 'New Retention Category' dialog box is shown. It has a title bar with a close button (X). The main area contains the following text:

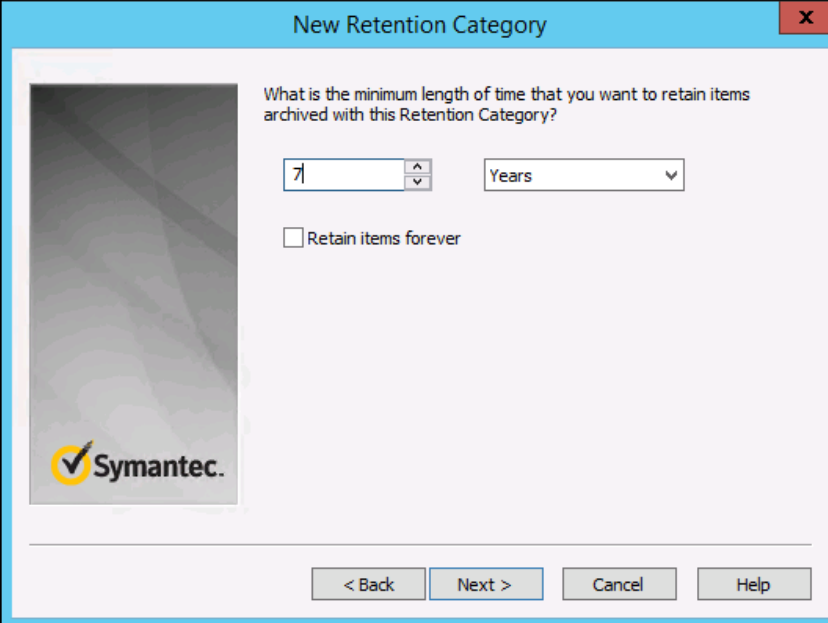
Enter a name and description for the new Retention Category.
The user sees this name and description when choosing a Retention Category, so make sure they are meaningful.

Name:

Description:

The Symantec logo is visible in the bottom left corner of the dialog. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Select the length of time you wish to retain items for this category.

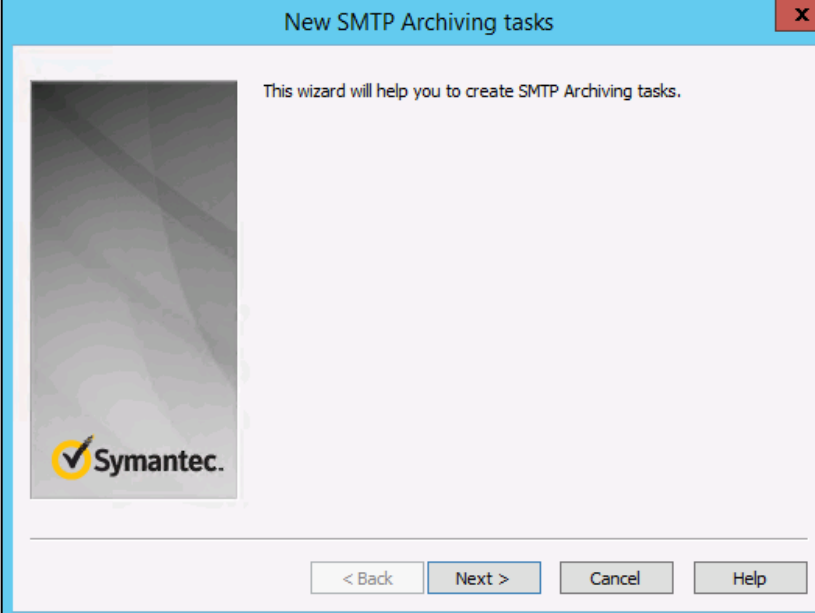


The dialog box is titled "New Retention Category" and features a close button (X) in the top right corner. On the left is a greyed-out image of a document with the Symantec logo at the bottom. The main text asks, "What is the minimum length of time that you want to retain items archived with this Retention Category?". Below this is a numeric input field containing "7", a small up/down arrow, and a dropdown menu set to "Years". A checkbox labeled "Retain items forever" is present and unchecked. At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

Click Finish to complete the wizard.

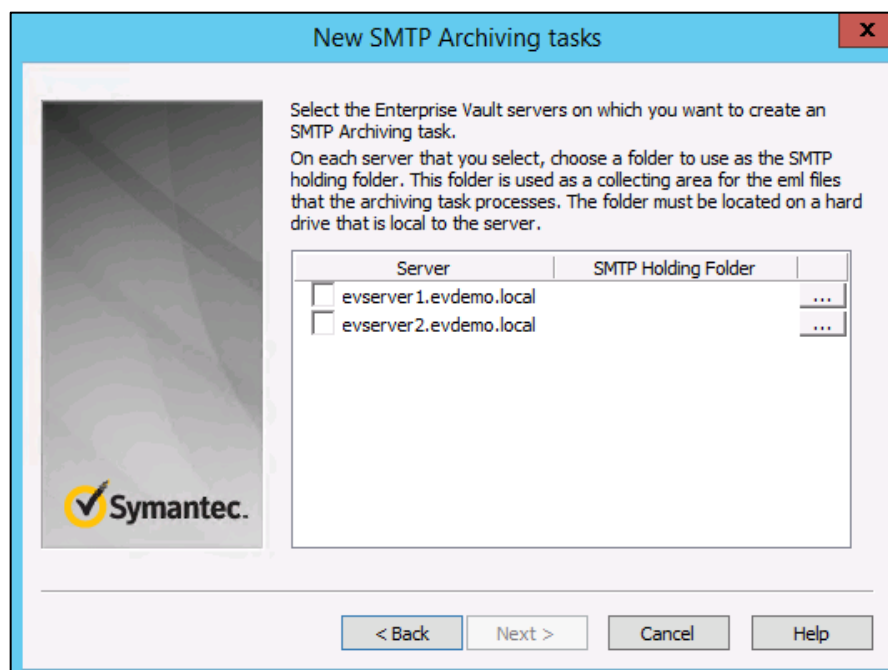
Create the EV SMTP Archiving Task.

Right-click on the Tasks container, choose SMTP Task. This wizard will also automatically start after creating the first SMTP target – if you've created the tasks already skip this step.

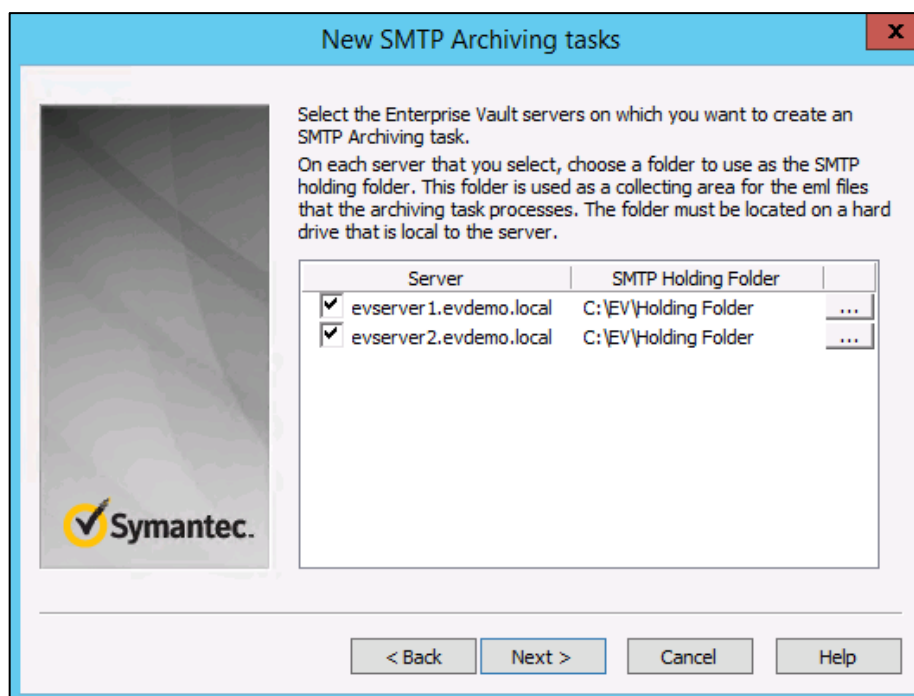


The dialog box is titled "New SMTP Archiving tasks" and has a close button (X) in the top right corner. On the left is a greyed-out image of a document with the Symantec logo at the bottom. The main text states, "This wizard will help you to create SMTP Archiving tasks." At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

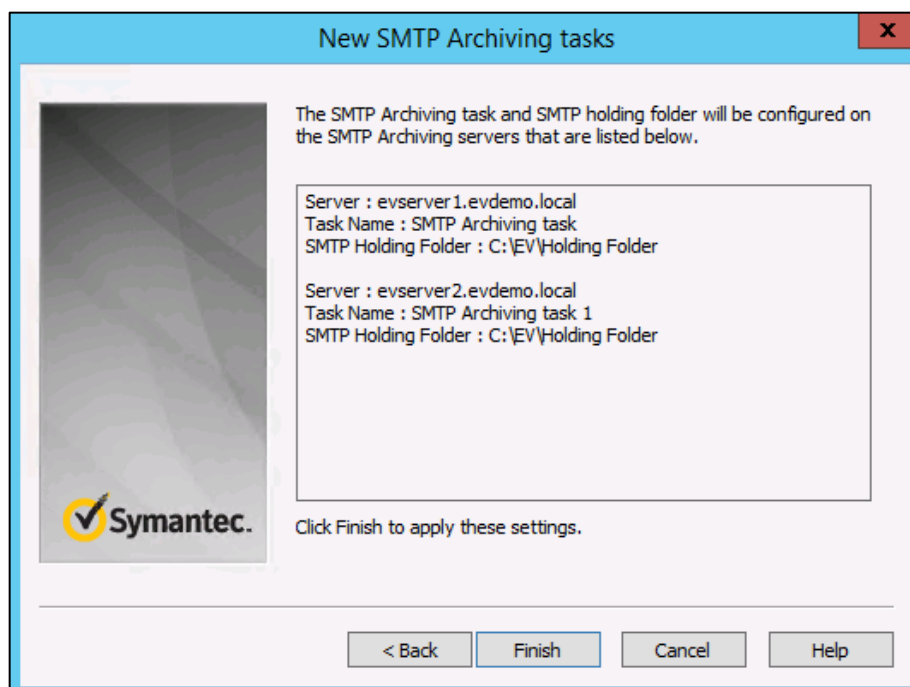
Click Next.



Select the server where you want to create the SMTP archiving task, and configure the holding folder location.



Note that in this particular example the C drive was selected as that was the only available drive, but in production environments it is recommended that the holding folder is stored on a fast, fault tolerant drive on a dedicated spindle set.



Click Finish to complete the wizard.

Click on the Tasks container and confirm both servers have the SMTP Archiving task running.

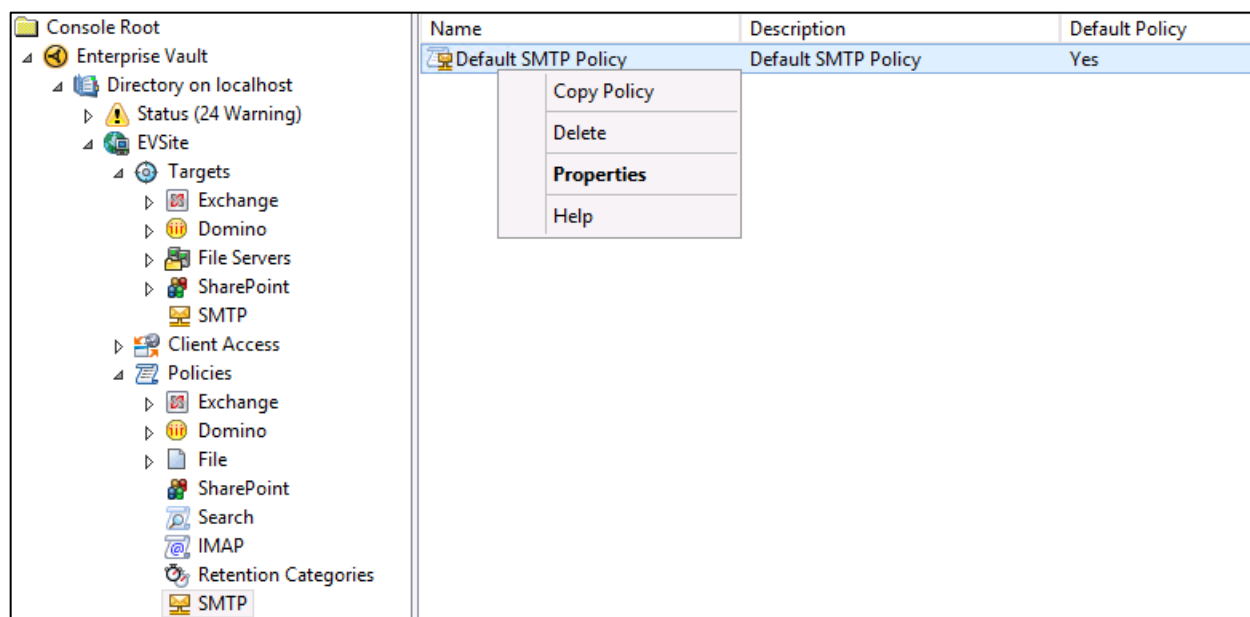
Console Root	Name	Type	Exchange Server	Status	Startup type
<ul style="list-style-type: none"> Enterprise Vault <ul style="list-style-type: none"> Directory on localhost <ul style="list-style-type: none"> Status (24 Warning) EVSite <ul style="list-style-type: none"> Targets <ul style="list-style-type: none"> Exchange Domino File Servers SharePoint SMTP Client Access Policies Enterprise Vault Servers <ul style="list-style-type: none"> evserver1.evdemo.local (:) <ul style="list-style-type: none"> Services Tasks evserver2.evdemo.local (:) <ul style="list-style-type: none"> Services Tasks Archives 	SMTP Archiving task	SMTP Archiving	N/A	Processing	Automatic

If operational the task will display "Processing" as status.

Configure the SMTP Policy

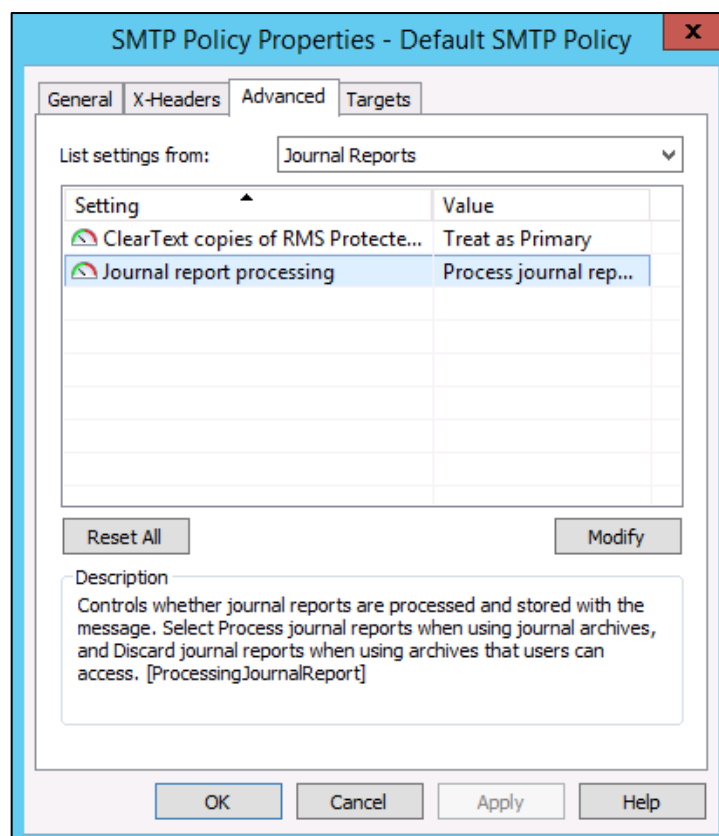
In this example the administrator will use the default SMTP Policy.

Right-click on the policy and select Properties.



If required add appropriate X-Header configuration (see earlier section in this document for more information).

Click on the Advanced tab.



Click on “Journal report processing”. For traditional SMTP journaling confirm that the setting is configured to “Process journal reports”, as this will capture the email wrapped in its Exchange envelope with relevant P1 header information.

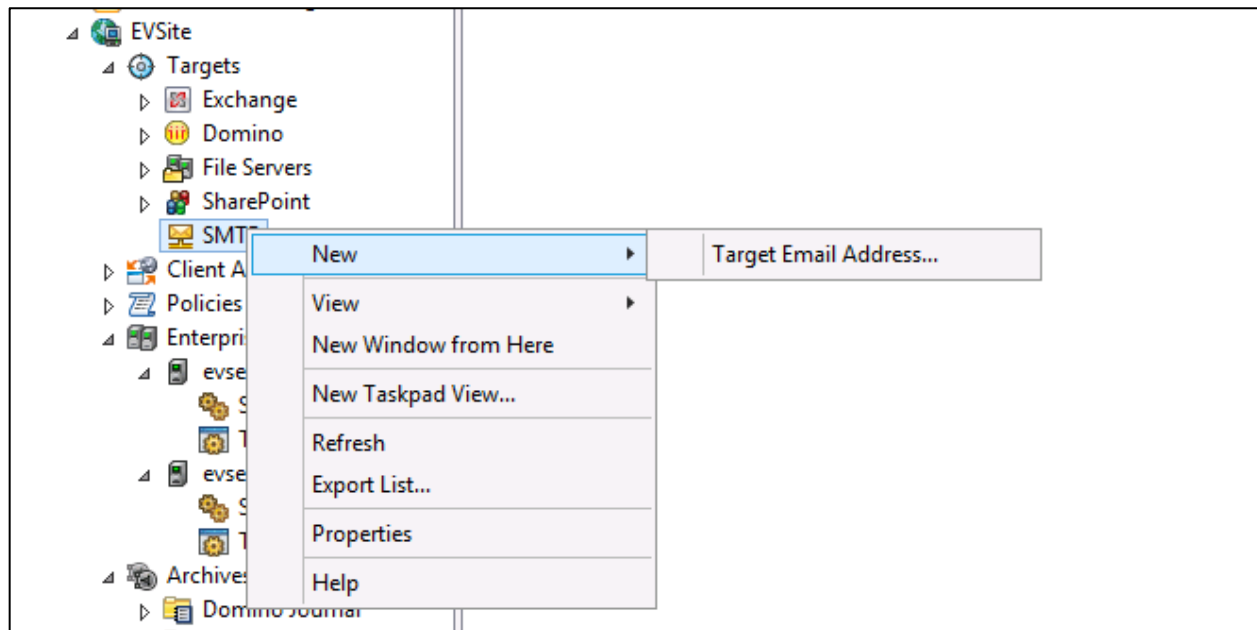
For SMTP Mailbox Journaling or Selective SMTP Journaling where the administrator may wish to give end user access to personal or shared journal archives, select the option to “Discard Journaling Reports”. The difference is that end users will see the original item when they open the message, rather than the contents of the envelope message (which will require the end user to double-click on the message again to see the message body or any attachments).

Click OK to close the properties window.

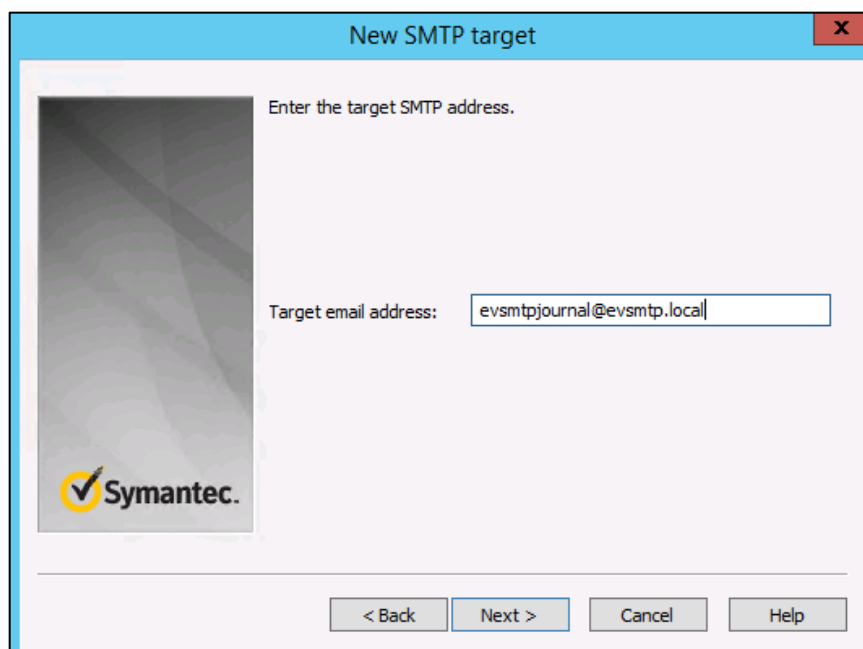
Create the SMTP Target addresses

The Enterprise Vault SMTP server will only accept addresses that are explicitly configured. In this example the administrator will configure Exchange to journal all email to the address evsmtpjournal@evsmtp.local. This is therefore the first address that should be configured as an accepted target.

Right-click on the SMTP container under Targets, and create a new Target Email Address.

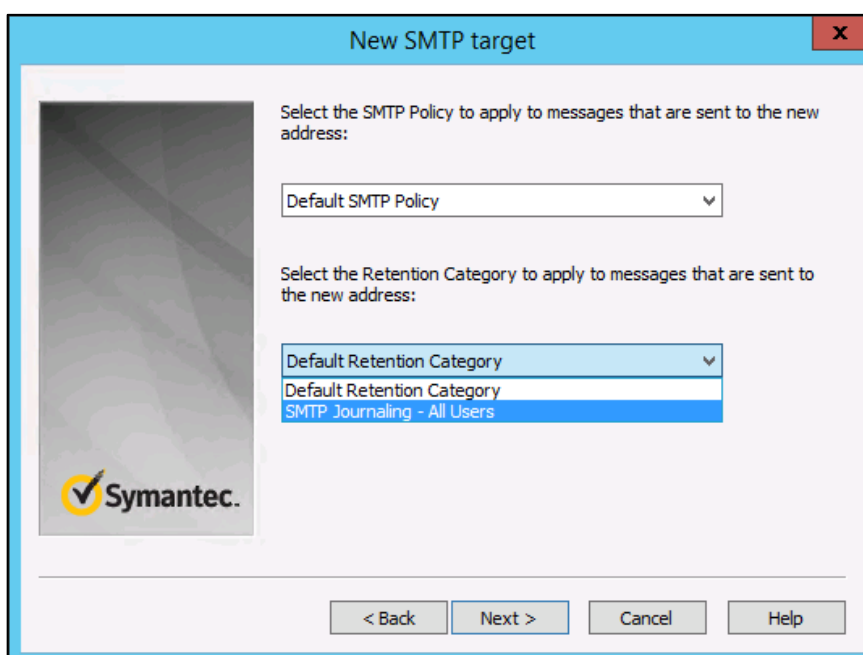


Enter the address evsmtpjournal@evsmtp.local.



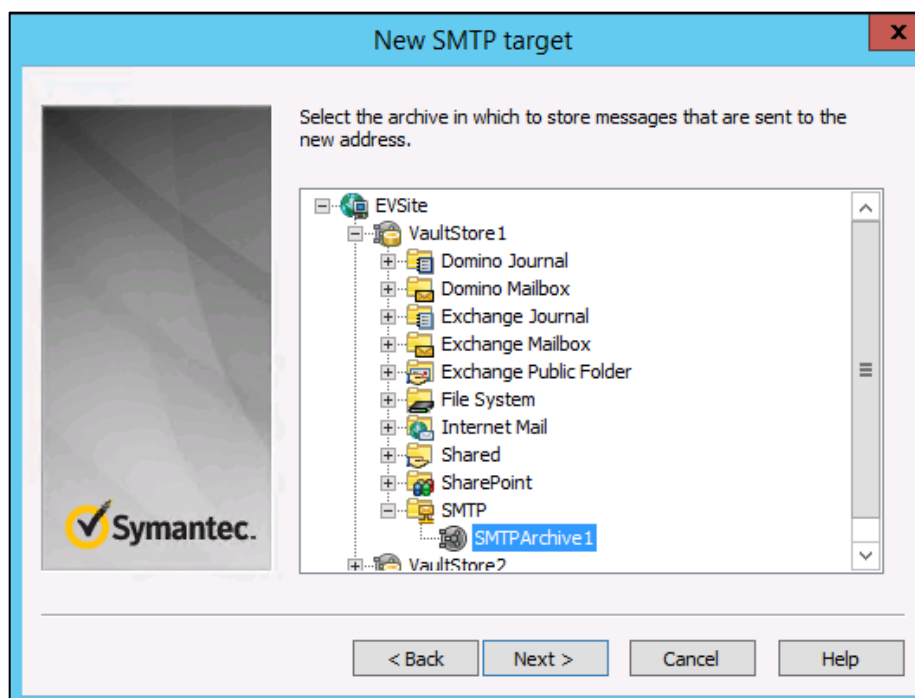
The dialog box is titled "New SMTP target" and features the Symantec logo on the left. The main area contains the instruction "Enter the target SMTP address." and a text input field labeled "Target email address:" with the value "evsmtpjournal@evsmtp.local". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

Click Next and select the SMTP Retention Category.



The dialog box is titled "New SMTP target" and features the Symantec logo on the left. The main area contains the instruction "Select the SMTP Policy to apply to messages that are sent to the new address:" followed by a dropdown menu showing "Default SMTP Policy". Below this, it says "Select the Retention Category to apply to messages that are sent to the new address:" followed by a dropdown menu. The dropdown menu is open, showing "Default Retention Category" and "SMTP Journaling - All Users". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

Click Next, and select an archive as default destination for the SMTP target.



Click Next and Finish to complete the wizard.

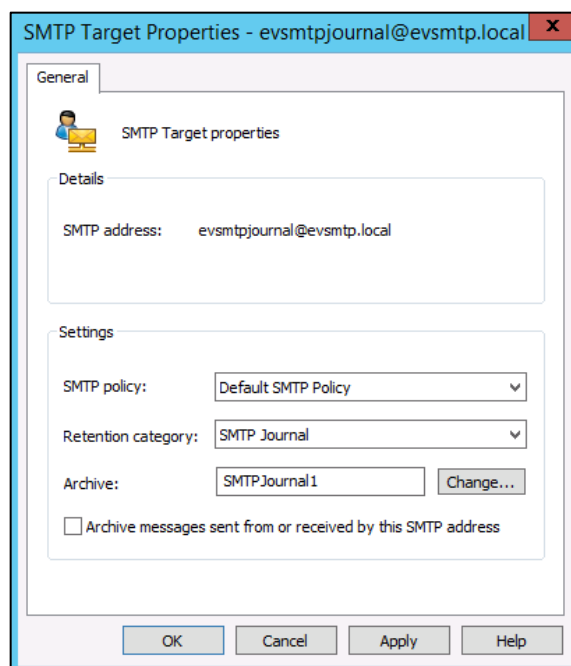
At this point the journal address evsmtpjournal@evsmtp.local is only associated with one archive, SMTPArchive1. The Vault Admin Console only allows you to configure one destination archive per target email address. If the administrator were to enable journaling on Exchange at this point, email will be evenly distributed to both EVServer1 and EVServer2, but the SMTP Archiving Task on EVServer2 will have to push the email via the CM API to EVServer1 as that is where the archive is hosted for that address. The Exchange server and the load balancing mechanism have no concept of the address only being associated with EVServer1. See Fan-out and Address Rewriting section for more information on this feature.

In order to distribute the workload evenly across both EV servers and utilize both storage services, a further two email address targets will be created. evsmtp1@evsmtp.local will be created and associated with the SMTPJournal1 archive, and evsmtp2@evsmtp.local will be created and associated with SMTPJournal2.

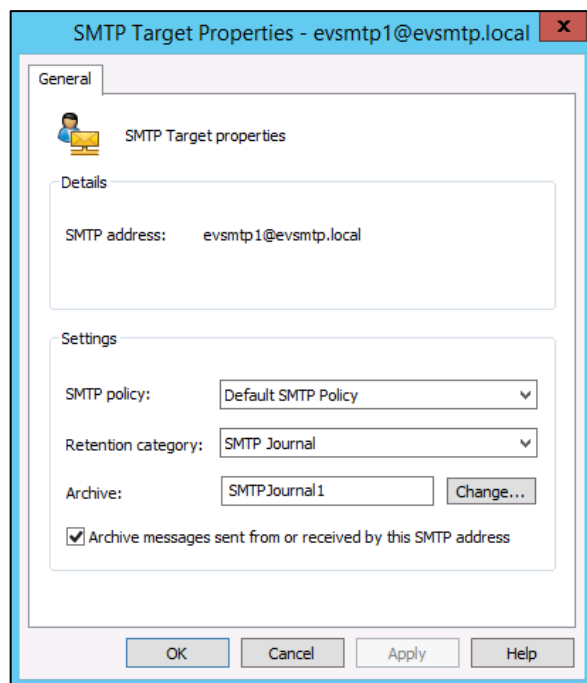
Use the New Target wizard now to create the two target addresses. When completed the configuration should be as follows:

Target Email Address	Domain	Policy	Retention Category	Archive	Vault Store
evsmtpjournal@evsmtp.local	evsmtp.local	Default SMTP ...	SMTP Journal	SMTPJournal1	VaultStore1
evsmtp1@evsmtp.local	evsmtp.local	Default SMTP ...	SMTP Journal	SMTPJournal1	VaultStore1
evsmtp2@evsmtp.local	evsmtp.local	Default SMTP ...	SMTP Journal	SMTPJournal2	VaultStore2

Now double-click on evsmtpjournal@smtp.local to bring up the target properties. As this is a routing address (in other words the server won't actually archive this address, it will archive the evsmtp1@evsmtp.local and evsmtp2@evsmtp.local addresses) clear the box next to "Archive messages sent or received by this SMTP address).



Ensure both evsmtp1@evsmtp.local and evsmtp2@evsmtp.local target addresses have the check box "Archive messages sent from or received by this SMTP address" selected.

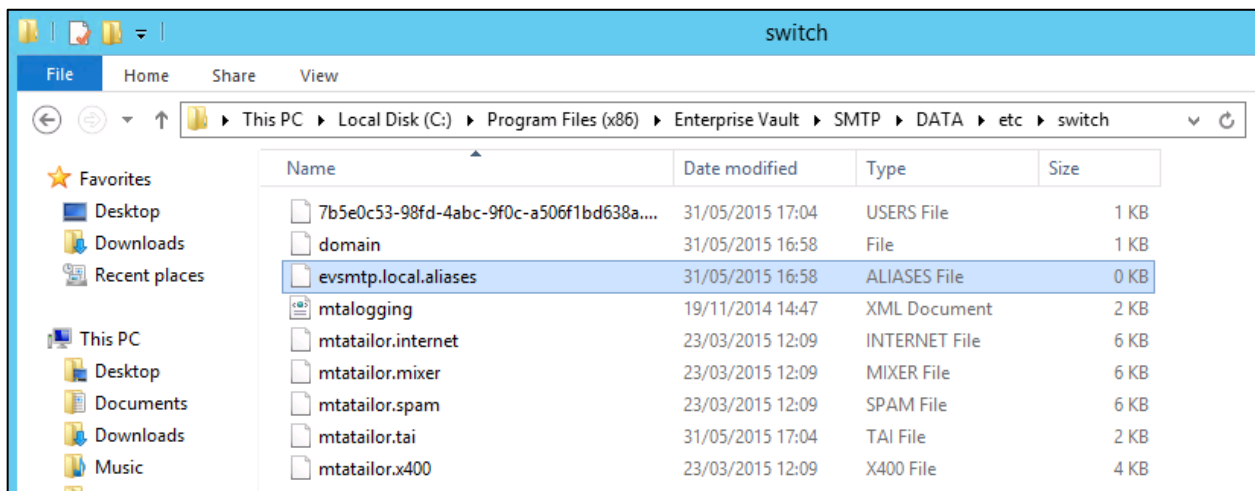


Restart the Enterprise Vault SMTP Service on both EVServer1 and EVServer2 for the changes to take effect.

Configuring Address Rewriting

On EVServer1 address rewriting will be configured to rewrite evsmtpjournal@evsmtp.local to evsmtp1@evsmtp.local, and on EVServer2 address rewriting will be configured to rewrite evsmtpjournal@evsmtp.local to evsmtp2@evsmtp.local.

For each email domain that the administrator creates a target address for, an alias file automatically gets created in the <Enterprise Vault Install>\SMTP\Data\etc\switch folder on every Enterprise Vault SMTP Server.



Any changes the administrator makes to this file will remain local to that particular server.

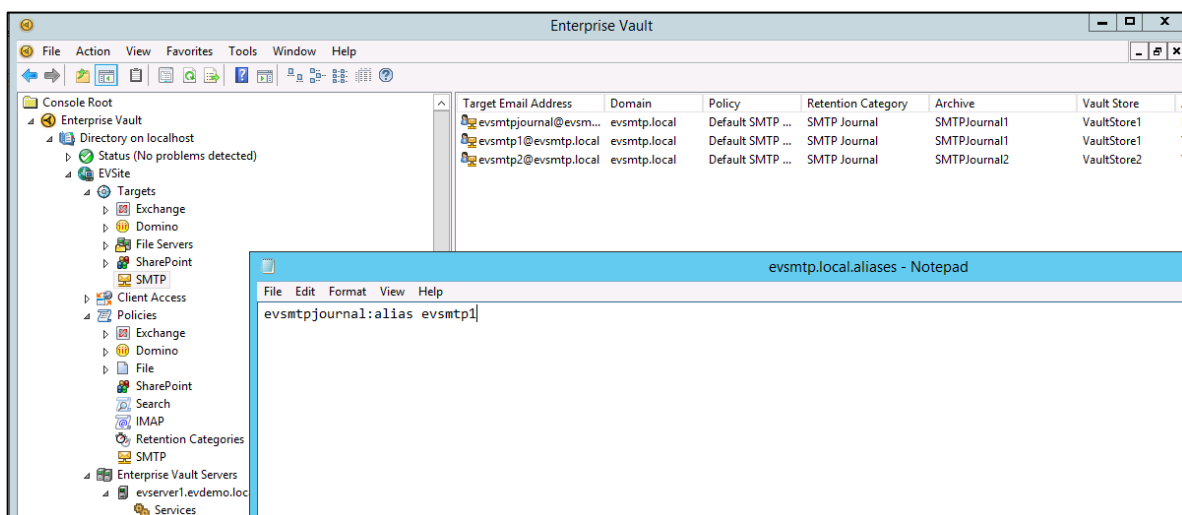
To edit the file, open with Notepad or any equivalent text editor.

Add the alias entry in the following format:

```
Incoming_name:alias rewrite_name
```

For this scenario add the following entry for EVServer1:

```
Evsmtjournal:alias evsmtp1
```



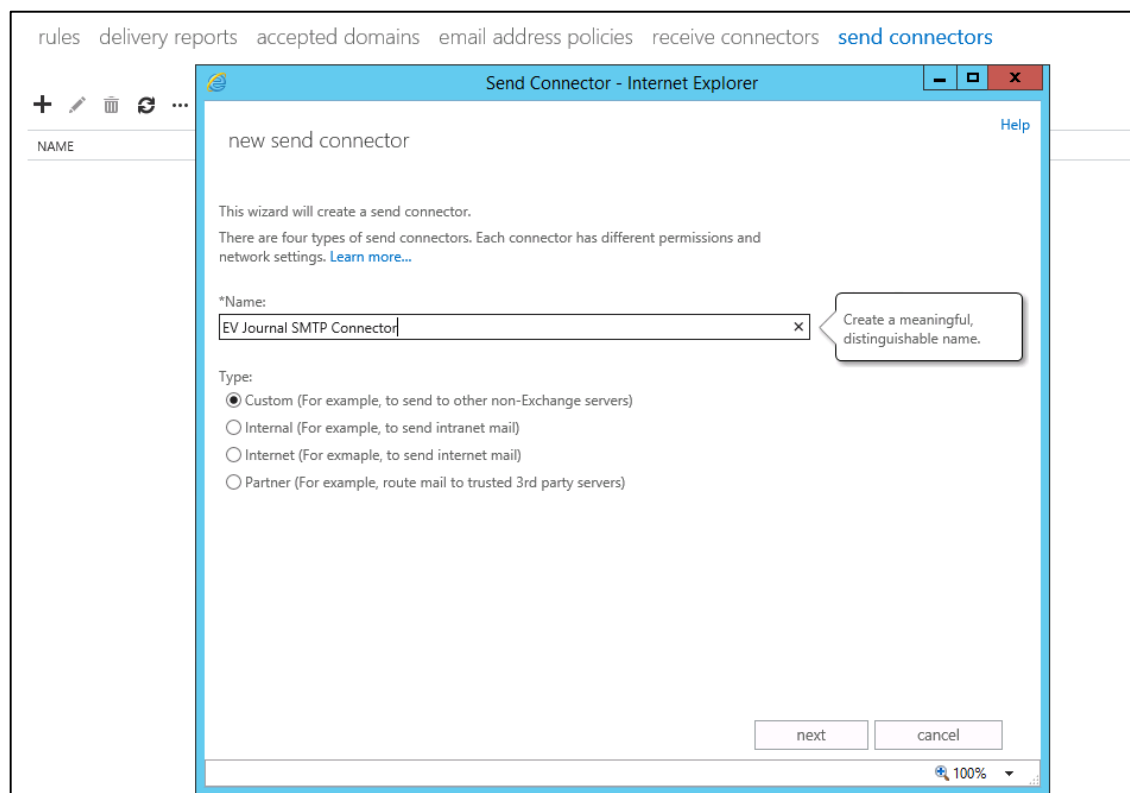
Log onto EVServer2 and add the following entry: `Evsmtplibjournal:alias evsmtp2`

If Windows folder access is denied, copy the file elsewhere, modify the contents and then copy back to the folder, overwriting the original version. Ensure that the file extension is “.aliases”, not “.txt”. (change the File Explorer view options to show file extensions for known file types).

Save the file, and restart the Enterprise Vault SMTP service.

Appendix D Creating a Send Connector with Multiple Smart Hosts in Exchange 2013

Click the “+” in the Send Connector tab to start the New Send Connector wizard. Enter an appropriate name for the connector, leave the Type on “Custom” and click Next.



Select the “Route mail through smart hosts” radio button, and add the EV SMTP server IP addresses by using the “+” sign.

new send connector

A send connector can route mail directly through DNS or redirect it to a smart host. [Learn more...](#)

*Network settings:
Specify how to send mail with this connector.

☐ MX record associated with recipient domain
☒ Route mail through smart hosts

+ -

SMART HOST

192.168.0.105

192.168.0.103

☐ Use the external DNS lookup settings on servers with transport roles

back next cancel

100%

On the next screen choose encryption option if required, and click Next.

new send connector

Configure smart host authentication. [Learn more...](#)

Smart host authentication:

☒ None
☐ Basic authentication
☐ Exchange server authentication

☐ Offer basic authentication only after starting TLS

*User name:

*Password:

Note: all smart hosts must accept the same username and password.

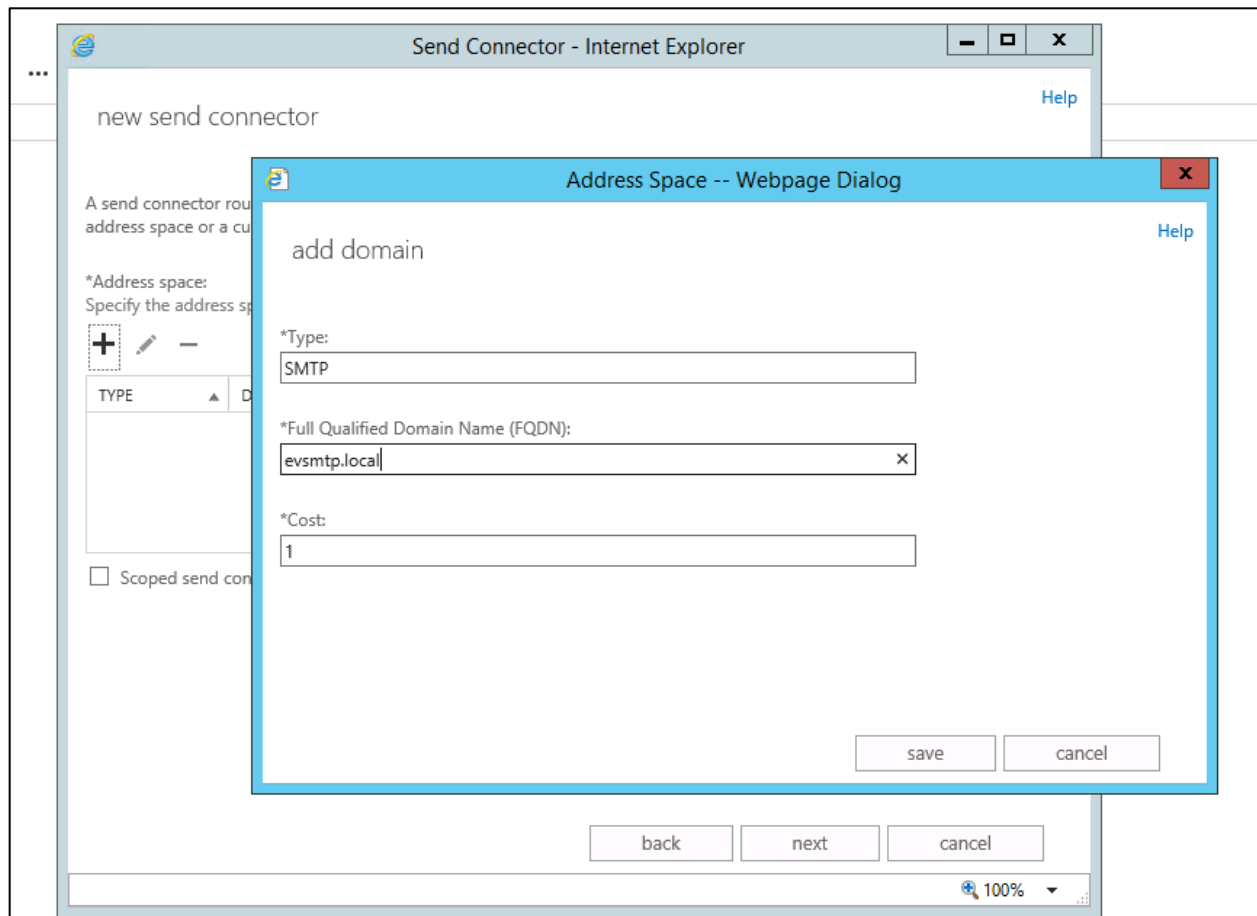
☐ Exchange server authentication
☐ Externally secured (for example, with IPSec)

back next cancel

100%

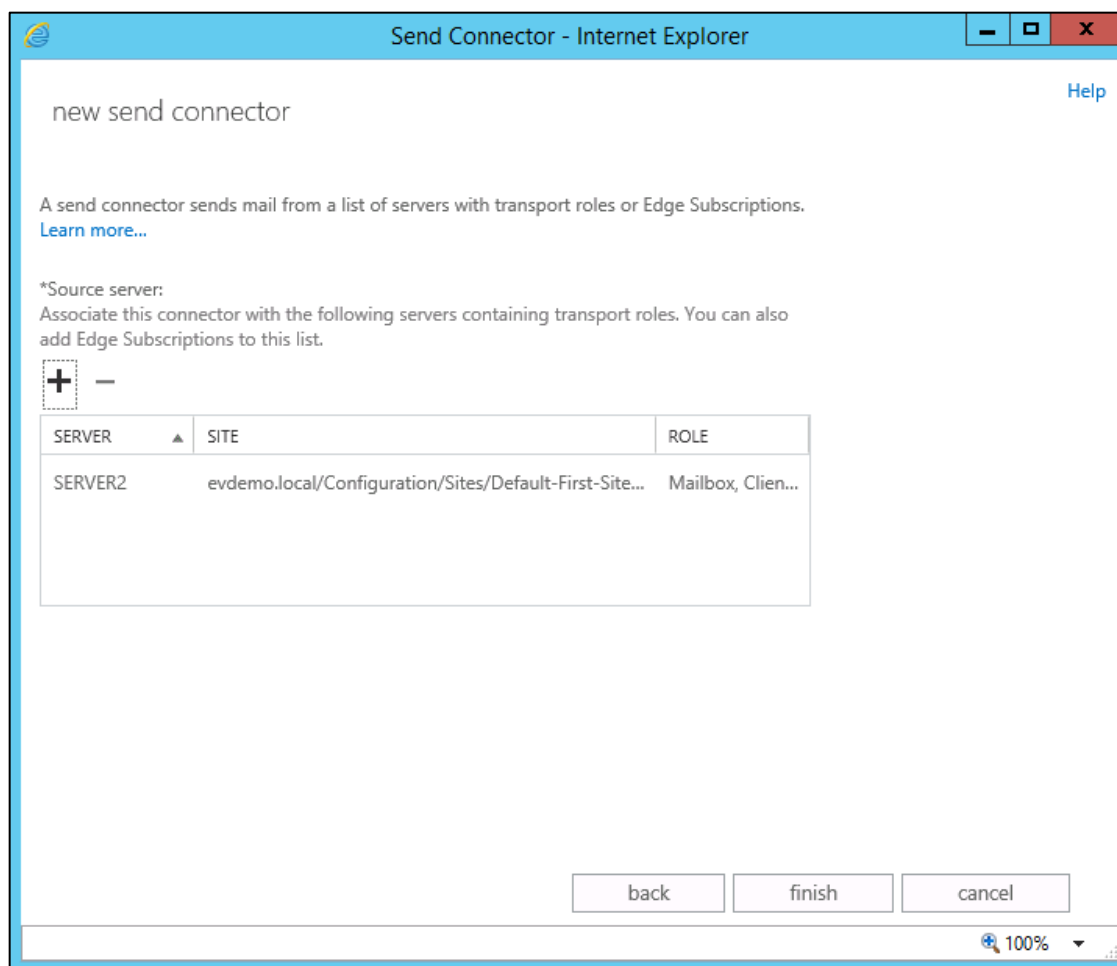
Add the domain name of the email address intended for routing the SMTP traffic to the Enterprise Vault SMTP server. Note that this address cannot be an existing known domain in the Exchange organization, and this connector should be the only connector responsible for routing this domain. If using smart hosts to route the email there is no requirement to configure a DNS Zone for the SMTP domain.

Click Save, followed by Next.



The next step is to add the Exchange Servers allowed to use this Send Connector. The choice of servers is dependent on the configuration and geographic location of Exchange Servers within the organization. Consult with the Exchange administrator and carefully consider the impact any server choices may have on network bandwidth and server resources.

It is recommended that at least two Exchange servers are allowed to use this connection to avoid any queue build up should one server be unavailable.



Click Finish to close the wizard.

Now double-click the connector to edit the properties. The default maximum message size for the connector is 10MB – this is not sufficient for most organizations. Choose an appropriate maximum size. Confirm the details are correct on the other tabs, and click Save.

At this point Exchange is configured to send email to the Enterprise Vault servers – do not enable Journaling until the Enterprise Vault servers are fully configured to receive SMTP traffic.

Exchange Send Connector - Internet Explorer

EV Journal SMTP Connector [Help](#)

► **general**
delivery
scoping

*Name:
EV Journal SMTP Connector

Connector status:
☒ Enable
☐ Proxy through client access server

Comment:

Protocol logging level:
☒ None
☐ Verbose

*Maximum send message size (MB):
10

Valid range is 0 to 2096128.

save cancel

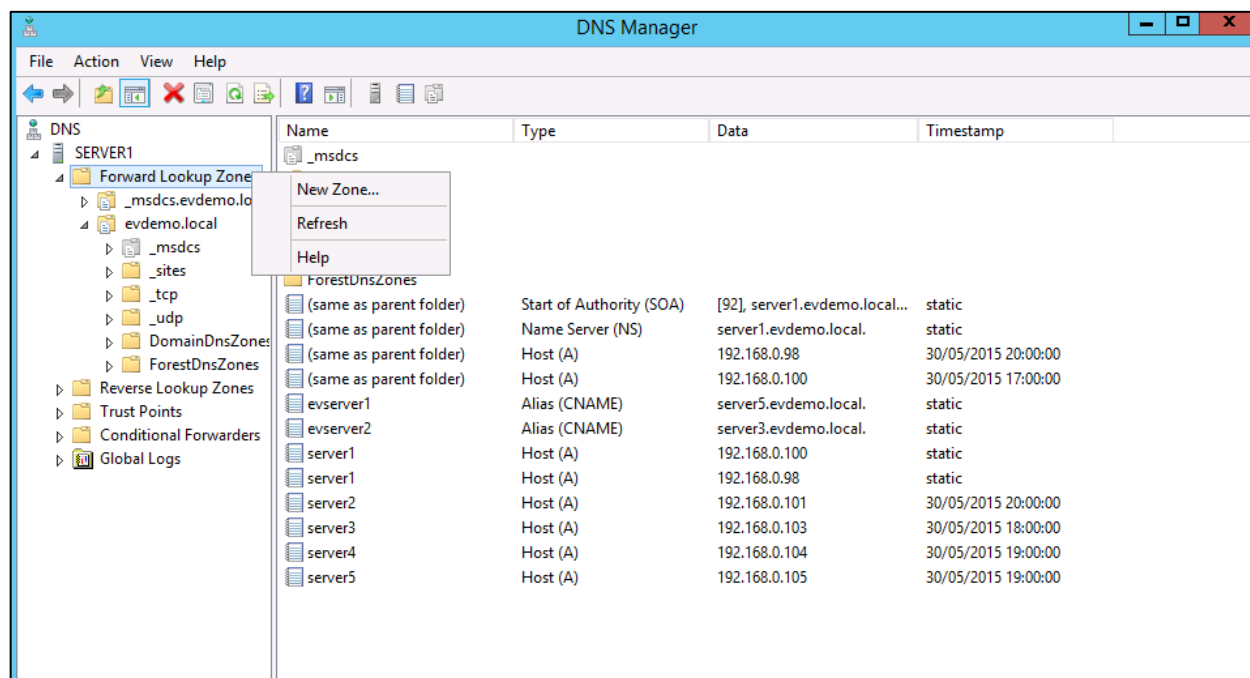
100%

Appendix E Creating a Send Connector using MX Records for Exchange 2013

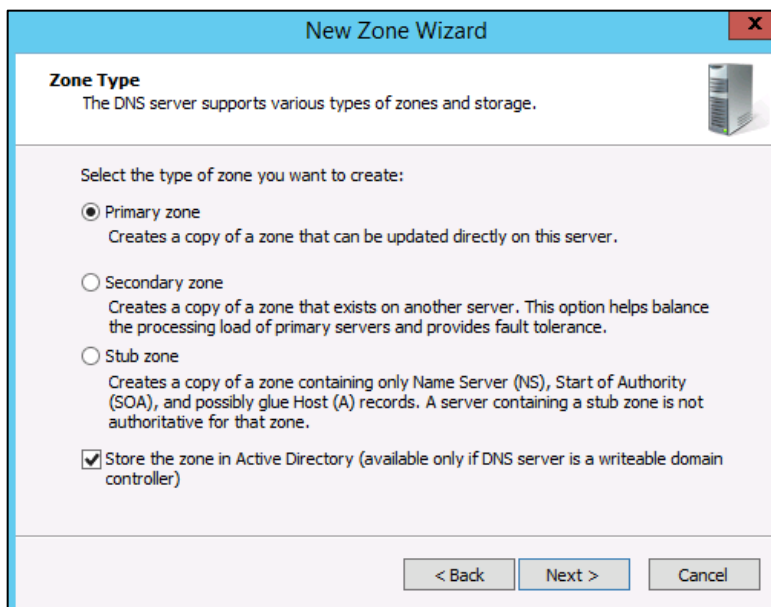
Because DNS is used by the sending mail server to query MX records, the first step is to create a Forward Lookup DNS Zone for the domain you intend to use for SMTP mail delivery to the Enterprise Vault servers.

This example uses Active Directory DNS – to start the configuration log in with the appropriate Administrator level account and open the DNS Manager console.

Right-click on the Forward Lookup Zone, and choose “New Zone”.



Select the type of zone as “Primary Zone” and click Next.



The screenshot shows the 'New Zone Wizard' window with the 'Zone Type' tab selected. The title bar reads 'New Zone Wizard' with a close button. Below the title bar, the text 'Zone Type' is followed by 'The DNS server supports various types of zones and storage.' To the right is a server icon. The main area contains the instruction 'Select the type of zone you want to create:' followed by three radio button options: 'Primary zone' (selected), 'Secondary zone', and 'Stub zone'. Each option has a descriptive text block. Below these is a checked checkbox labeled 'Store the zone in Active Directory (available only if DNS server is a writeable domain controller)'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Zone Type
The DNS server supports various types of zones and storage.

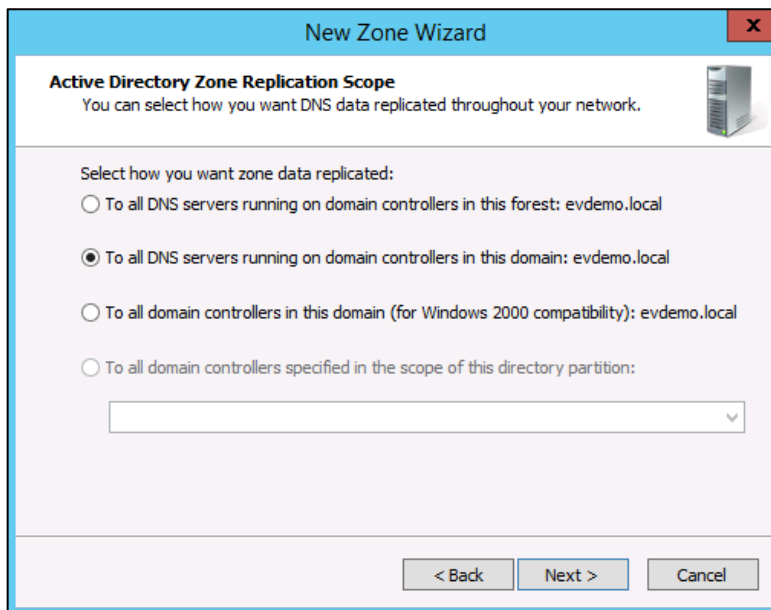
Select the type of zone you want to create:

- ☒ **Primary zone**
Creates a copy of a zone that can be updated directly on this server.
- ☐ **Secondary zone**
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ **Stub zone**
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☒ **Store the zone in Active Directory** (available only if DNS server is a writeable domain controller)

< Back Next > Cancel

Choose the appropriate propagation setting for your DNS domain and click Next.



The screenshot shows the 'New Zone Wizard' window with the 'Active Directory Zone Replication Scope' tab selected. The title bar reads 'New Zone Wizard' with a close button. Below the title bar, the text 'Active Directory Zone Replication Scope' is followed by 'You can select how you want DNS data replicated throughout your network.' To the right is a server icon. The main area contains the instruction 'Select how you want zone data replicated:' followed by four radio button options, each with a text block: 'To all DNS servers running on domain controllers in this forest: evdemo.local', 'To all DNS servers running on domain controllers in this domain: evdemo.local' (selected), 'To all domain controllers in this domain (for Windows 2000 compatibility): evdemo.local', and 'To all domain controllers specified in the scope of this directory partition:' followed by a dropdown menu. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

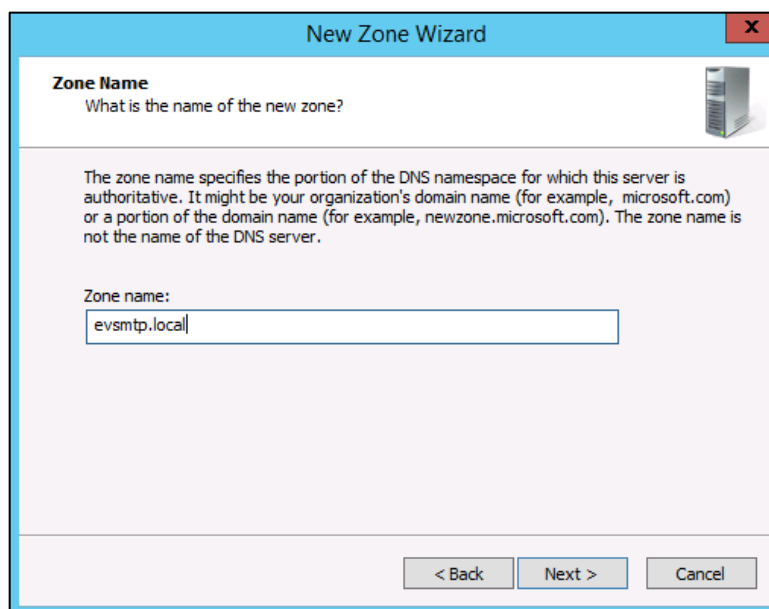
Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

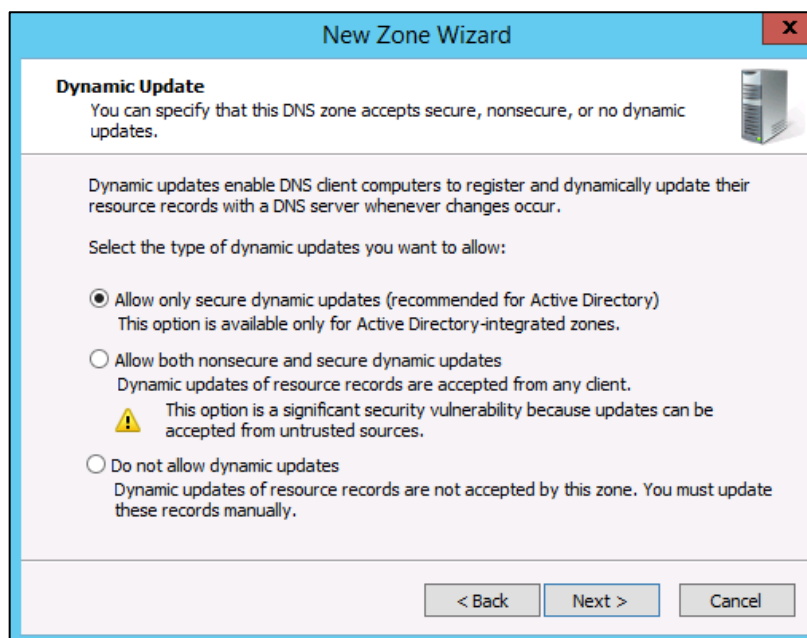
- ☐ To all DNS servers running on domain controllers in this forest: evdemo.local
- ☒ To all DNS servers running on domain controllers in this domain: evdemo.local
- ☐ To all domain controllers in this domain (for Windows 2000 compatibility): evdemo.local
- ☐ To all domain controllers specified in the scope of this directory partition:

< Back Next > Cancel

Specify the name of the DNS zone that will be used to route the journal emails.

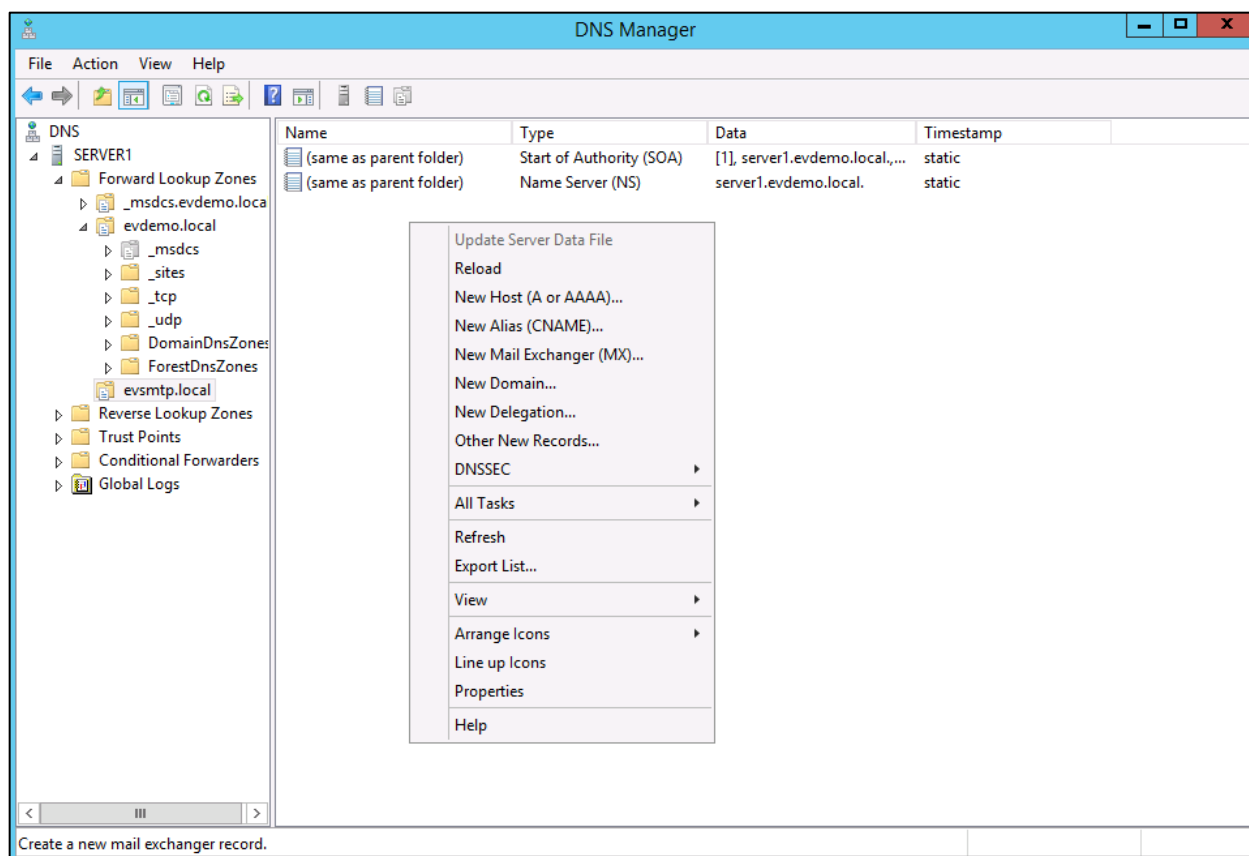


Select the appropriate security update setting for your environment and click Next. Close the wizard.



Now create the MX records for the Enterprise Vault SMTP servers. Only create entries for the servers you wish to receive SMTP traffic.

Right-click on the appropriate domain, and choose the “New Mail Exchanger (MX)” record option.



Leave the “Host or child domain” entry blank. Enter the FQDN of the Enterprise Vault SMTP server, or click Browse to locate the server in the DNS zone that the server is a member of.

Leave the mail server priority at 10, and click OK to close the wizard.

New Resource Record

Mail Exchanger (MX)

Host or child domain:

By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.

Fully qualified domain name (FQDN):

evsmtp.local.

Fully qualified domain name (FQDN) of mail server:

server3.evdemo.local Browse...

Mail server priority:

10

OK Cancel Help

Now create further MX records for the remaining Enterprise Vault SMTP servers, ensuring all servers are configured with the same mail server priority as that will enable the load balancing algorithm in the Exchange Send connector to evenly distribute email across the servers.

New Resource Record

Mail Exchanger (MX)

Host or child domain:

By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.

Fully qualified domain name (FQDN):

evsmtp.local.

Fully qualified domain name (FQDN) of mail server:

server5.evdemo.local Browse...

Mail server priority:

10

OK Cancel Help

Now open the Exchange Admin Center, and locate the Send Connector tab. Create a new Connector using the same steps provided in the previous Smart Hosts section of this document, except this time choose “MX record associated with the recipient domain”.

Exchange Send Connector - Internet Explorer

EV SMTP Journal

general
▶ delivery
scoping

*Network settings:
Specify how to send mail with this connector.

☒ MX record associated with recipient domain
☐ Route mail through smart hosts

+ ✎ -

SMART HOST

Smart host authentication:

☒ None
☐ Basic authentication
☐ Offer basic authentication only after starting TLS

*User name:
[Text Box]

*Password:
[Text Box]

Note: all smart hosts must accept the same username and password.

save cancel

100%

Confirm all settings including message sizes in the Send Connector properties and save any changes.

Appendix F End to End SMTP Message Tracking for Exchange Journal Archiving

This section will explain end-to-end email flow from the Exchange server to the journal archive in Enterprise Vault.

The following high-level diagram details the process.

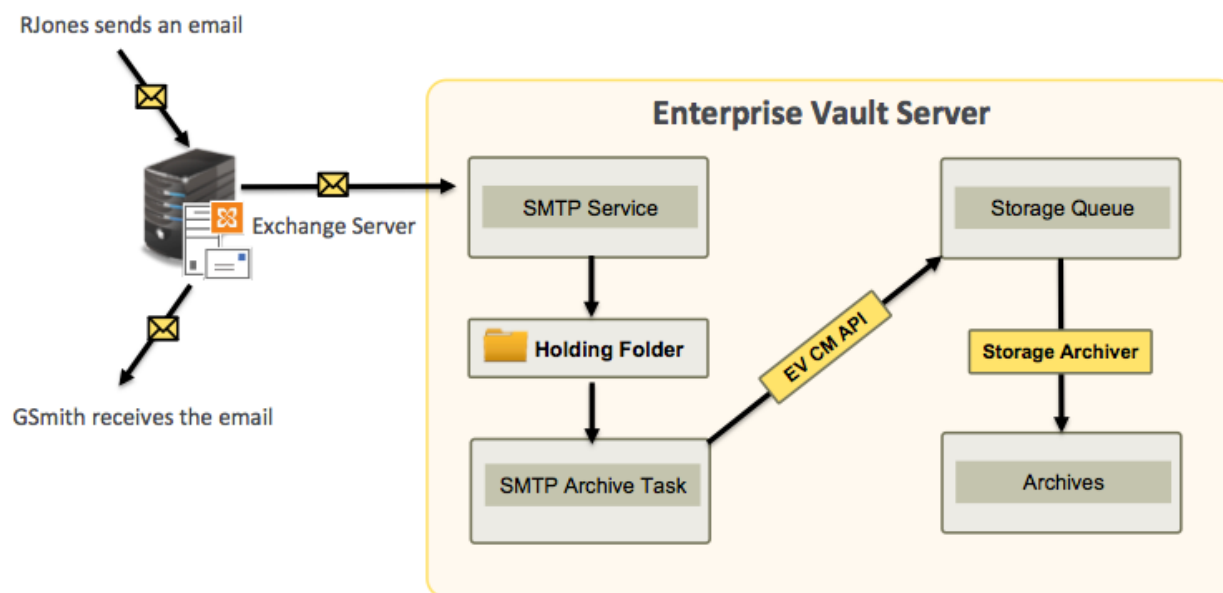


Figure 24 – High-level SMTP Journal Message Flow

The mail flow can be divided in following sub systems:

- Exchange server
- SMTP server
- Holding Folder
- SMTP Archiving Task
- Storage Queue
- Archives

The following section covers each sub system in detail.

Exchange Server

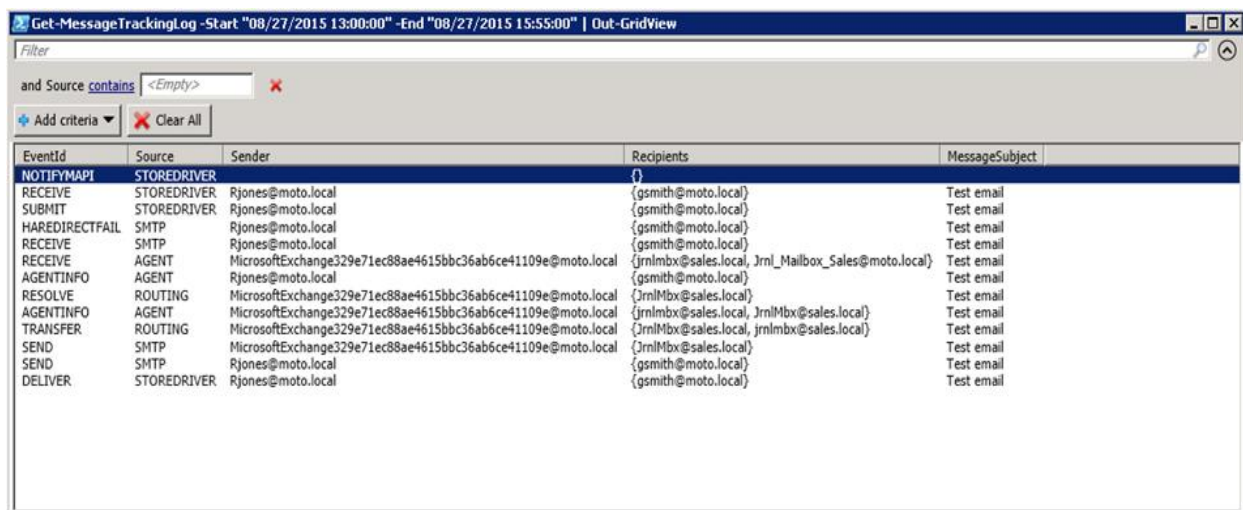
Microsoft Exchange provides both standard and premium journaling options to journal email. The Journal recipient can either be a mailbox or an SMTP contact email address. By using a contact with an email address that is external from the organization, the administrator can create a SMTP Send Connector to deliver journal mail directly to the EV SMTP server.

In the above example, Rjones@moto.local and Gsmith@moto.local are mailboxes on the Exchange server. A journaling target email address Journaling@evsmtp.local is created on EV SMTP server. When an email is sent from Rjones@moto.local to Gsmith@moto.local, a copy of the journal email is sent to Journaling@evsmtp.local.

Message Tracking at the Exchange Server

The following figure shows how Exchange tracks the message from when the email is sent to the recipient mailbox, and the journal copy is relayed to the EV SMTP server. Use the following PowerShell command to view the log:

Get-MessageTrackingLog | Out-GridView



EventId	Source	Sender	Recipients	MessageSubject
NOTIFYMAPI	STOREDRIVER	Rjones@moto.local	{}	
RECEIVE	STOREDRIVER	Rjones@moto.local	{gsmith@moto.local}	Test email
SUBMIT	STOREDRIVER	Rjones@moto.local	{gsmith@moto.local}	Test email
HARDIRECTFAIL	SMTP	Rjones@moto.local	{gsmith@moto.local}	Test email
RECEIVE	SMTP	Rjones@moto.local	{gsmith@moto.local}	Test email
RECEIVE	AGENT	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@moto.local	{JrnlMbx@sales.local, Jrnl_Mailbox_Sales@moto.local}	Test email
AGENTINFO	AGENT	Rjones@moto.local	{gsmith@moto.local}	Test email
RESOLVE	ROUTING	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@moto.local	{JrnlMbx@sales.local}	Test email
AGENTINFO	AGENT	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@moto.local	{JrnlMbx@sales.local, JrnlMbx@sales.local}	Test email
TRANSFER	ROUTING	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@moto.local	{JrnlMbx@sales.local, JrnlMbx@sales.local}	Test email
SEND	SMTP	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@moto.local	{JrnlMbx@sales.local}	Test email
SEND	SMTP	Rjones@moto.local	{gsmith@moto.local}	Test email
DELIVER	STOREDRIVER	Rjones@moto.local	{gsmith@moto.local}	Test email

Figure 25 – Exchange Message Tracking using Powershell

If the EV SMTP Server is not available, then messages are queued on the Exchange server until the SMTP Server is once again available. On the Exchange Server, look for the mail flow tool i.e. queue viewer which manages the undeliverable emails and troubleshoot error codes accordingly.

The figure 27 shows how messages are displayed when stuck in the Exchange queue viewer.

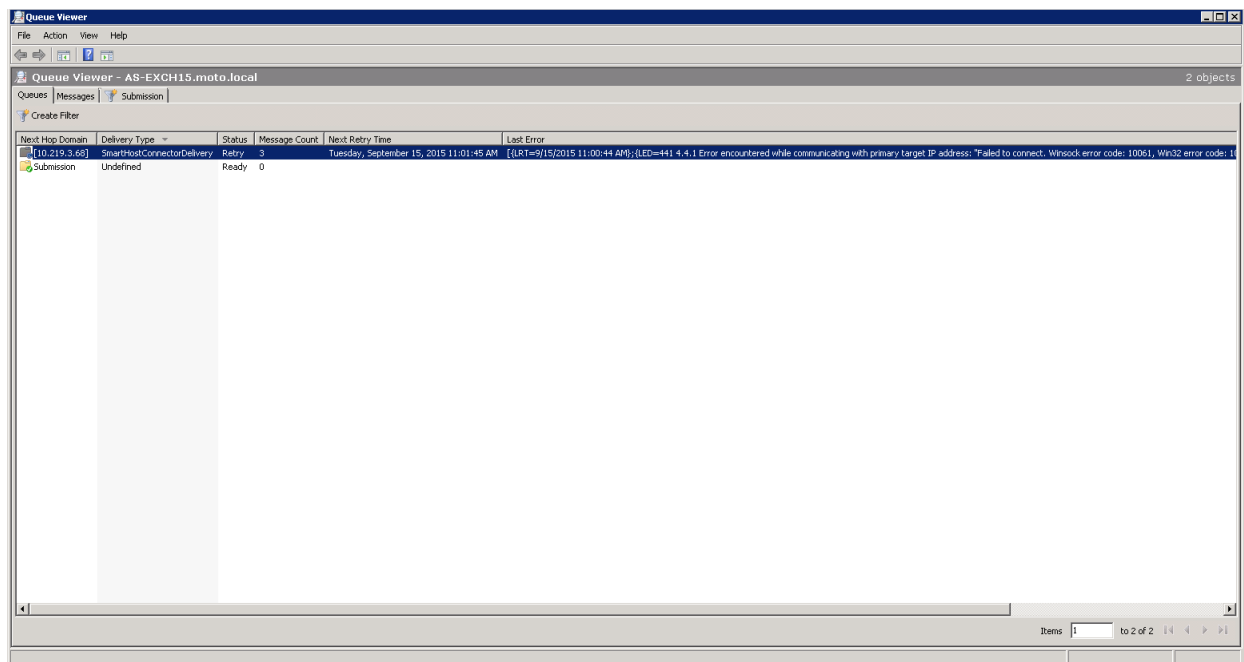


Figure 26 – Exchange Queue Viewer

Message Tracking at EV SMTP Server

At the EV SMTP server, the message first arrives in the Holding Folder. The SMTP server records the details of each message and acknowledgement. If Dtrace is enabled the details are logged to a file. The Dtrace log contains the following information about the message, which help administrator in the tracking the messages.

- Subject³
- Recipients
- Message Size
- Message Sender
- Message Status (delivered, rejected, etc.),

Following is an example of a typical Dtrace log:

```
2015-09-01 14:45:43 Enterpri 14888 (#0          ) ConnectFrom chan:smtp-external host:as-dc0-  
barfi0.moto.local ip:10.219.3.71
```

2015-09-01 14:45:43 Enterpri 14888 (#0) Archive unid:VeVswA6KBQB qid:msg.00000-0
file:"C:/SMTPHoldingFolder/01/09/15/1441098943.14888.1.eml"

2015-09-01 14:45:43 Enterpri 14888 (#0) Msgin unid:VeVsvwA6KBQB qid:msg.00000-0 type:User-Mpdu subject:"HSBC NFO getting lauched- bid" chan:smtp-external mta:as-dc0-barfi0.moto.local size:652 nrecip:1 content-type:822 sender:Rjones@moto.local submit-time:2015-09-01-14.45.43 queued-time:1970-01-01-05.30.00 priority:3

³ The subject will only be exposed in EV12 and later releases. In earlier releases the subject is masked

2015-09-01 14:45:43 Enterpri 14888 (#0) ok unid:VeVsvwA6KBQB qid:msg.00000-0 rno:1
 recip:gsmith@moto.local ureq:fwu mreq:0 chan:local mta:bogus

2015-09-01 14:45:43 Enterpri 14888 (#0) Disconnect chan:smtp-external host:as-dc0-barfi0.moto.local
 ip:10.219.3.71 helo:smtp.test.com

SMTP Server Performance Counter

In addition, the SMTP server can be monitored using performance counters, under the category "Enterprise Vault SMTP Service".

Concurrent connections - Number of concurrent connections to the Enterprise Vault SMTP service.

Connections rejected - Number of connections rejected by the Enterprise Vault SMTP service since the service was started.

SMTP messages original size (bytes) – Total original size of messages received by the Enterprise Vault SMTP service. (Bytes)

SMTP messages received - Number of SMTP messages received by the Enterprise Vault SMTP service since the service was started.

SMTP messages rejected - Number of SMTP messages rejected by the Enterprise Vault SMTP service since the service was started.

Enterprise Vault SMTP Service	
Concurrent connections	0.000
Connections rejected	0.000
SMTP messages original size (bytes)	652.000
SMTP messages received	1.000
SMTP messages rejected	0.000

Note: These counters will reset to zero when the SMTP service gets restarted.

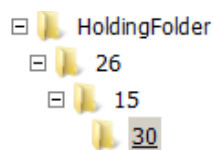
SMTP Holding Folder

The holding folder along with SMTP Server will reside on the Enterprise Vault Server.

The user context under which SMTP Server and SMTP Archiving task is running would have access to this folder. The holding folder may contain email for various recipients belonging to various domains. The folder structure is organized by time. An example is shown below:

E:\Mail Root (Holding Folder)

- 26 (day of month)
 - 15 (hour)
 - 30 (min)
 - 5cd6a8ba01cc51dd00000001.eml (actual emails)
 - 6feb03d801cc2f0f00000001.eml



SMTP Holding Folder Performance Counters

The SMTP holding folder can be monitored using performance counters, under category "Enterprise Vault SMTP Holding Folder".

Connectivity - Connectivity to the SMTP holding folder location. (Value of 0 for this counter indicates connectivity to holding folder could not be established and 1 indicates connectivity with holding folder can be established).

Disk space % used - Used space at the SMTP holding folder location.

Enterprise Vault SMTP Holding Folder	C:\SMTPHoldingFolder
Connectivity	1.000
Disk space % used	20.112

The eml files in the holding folder will be archived by the SMTP archiving task.

SMTP Archiving Task

The SMTP archiving task will be responsible for ingestion of emails received by the SMTP Server into the archive. SMTP Archiving Task would be operational 24x7.

The SMTP Archiving Task will be responsible for the following operations

- Enumerating emails received by SMTP Server from holding folder.
- Archiving emails as per the configured policy.
- Archiving emails along with index properties in appropriate archives using CM APIs.
- Moving failed eml files to the appropriate folder under the holding folder.
- Create Task summary report.
- Create Task error logs.
- Updating counters for reporting or monitoring and alerting.

SMTP task retrieves eml files from the holding folder. It parses recipients in *X-RCPT-TO* header and match with configured targets. If Selective Journal Archiving is configured the SMTP Archiving task parses all of the sender and recipient fields (*X-RCPT-TO*, *To*, *CC*, *BCC*, *From*, *Sender*) in each message.

If any recipient is matched, email will be archived using CM API. If an eml gets successfully stored in storage queue, it will be deleted from holding folder, "SMTP messages archived" and "SMTP messages processed" performance counters will be incremented. If SMTP archiving task is unable to archive eml, the file will be moved to "failed" folder, "SMTP messages unable to archive" and "SMTP messages processed" counters will be incremented.

Events in case of failure would be written to Event Log with sufficient detail and all the errors would be written to Task Error Log.

SMTP Task Error Log

All the errors in the SMTP Archiving task are logged in to the task error log. In addition to this a failure event would also be logged in the event log.

The error logs would be kept at "<Enterprise Vault Install Path>\Reports\SMTP\" folder. The name of the error file would be in format 'SMTPArchiving_Error_Log_
_<EV_SERVER_NAME>_<YYYYMMDD>_<HHmmSS>_<ms>_To_<YYYYMMDD>_<HHmmSS>_<ms>_
txt'

e.g. SMTPArchiving_Error_Log_Server1-EV-10_20130208_080602_97_To_20130209_010203_47.txt

The format and details for the error log file is as follows:

Event	Date	Time	File	Error code	Action Taken	Description
Unable to archive file	1/31/2013	11:46:02 AM	..\31\11\45\Multi.eml	0x80040303	Will be retried	User does not have sufficient rights on the archive or the archive is in a read-only state. Recipient: Rjones@moto.local
Unable to archive file	1/31/2013	1:17:04 PM	..\31\13\16\Successful1.eml	0x80040300	Will be retried	The Enterprise Vault Directory or Storage services are not running.
Unable to archive file	1/31/2013	1:48:03 PM	..\31\13\47\Successful3.eml	0x80040301	Will be retried	The target archive SMTPArchive is full or exceeds its quota limit.
Unable to archive file	1/31/2013	1:54:08 PM	..\31\13\53\Successful4.eml	0x80040302	Will be retried	Enterprise Vault is currently busy or has insufficient resource to complete the insertion
Unable to archive file	1/31/2013	2:23:02 PM	..\31\14\22\Failure3.eml	E_NO_RECIPIENTS_FOUND	File will be deleted	The eml file does not contain any recipients.
Unable to archive file	1/31/2013	2:23:02 PM	..\31\14\22\Failure4.eml	E_TARGET_NOT_CONFIGURED	File will be deleted	Target addresses did not match with any recipient.
Unable to move file to Archived folder	3/4/2013	10:41:02 AM	..\04\10\40\1342393637.5280.183.eml	112	Will be retried	There is not enough space on the disk.

Unable to archive file	3/4/2013	10:41:12 AM	..\04\10\40\1352393637.5280.193.em	0x80040305	File will be moved to Failed folder	Attempting to insert items into a structured archive containing multiple root folders
------------------------	----------	-------------	------------------------------------	------------	-------------------------------------	---

SMTP Task Summary Report Log

Each time the SMTP Archiving task starts it creates a new report file in the Reports\SMTP subfolder of the Enterprise Vault installation folder, for example C:\Program Files (x86)\Enterprise Vault\Reports\SMTP.

Date	Start Time	End Time	Archived	Processed	Unable To Archive	Size (MB)
06-08-2015	06:19 AM	07:00 AM	9731	9731	0	6.05
06-08-2015	07:00 AM	08:00 AM	22163	22163	0	13.78
06-08-2015	08:00 AM	09:00 AM	14998	14998	0	9.33
06-08-2015	09:00 AM	09:57 AM	22034	22034	0	13.7

SMTP Archiving Task Total Summary Information

Total messages processed: 68926

Total messages archived: 68926

Total messages unable to archive: 0

Total size messages archived (in MB): 42.86

SMTP Archiving Task Performance Counter

The SMTP archiving task can be monitored using performance counters, it will be under category "Enterprise Vault SMTP Archiving Task".

Maximum original size of SMTP messages (bytes) - Maximum original size of messages archived by the Enterprise Vault SMTP Archiving task. (Bytes).

SMTP messages archived - Number of SMTP messages archived by the Enterprise Vault SMTP Archiving task.

SMTP messages original size (bytes) - Total original size of messages archived by the Enterprise Vault SMTP Archiving task. (Bytes)

SMTP messages processed - Number of SMTP messages processed by the Enterprise Vault SMTP Archiving task. This includes data about SMTP messages that could not be archived.

SMTP messages unable to archive - Number of SMTP messages that the Enterprise Vault SMTP Archiving task is unable to archive.

Enterprise Vault SMTP Archiving Task	smtp archiving task
Maximum original size of SMTP messages (bytes)	652.000
SMTP messages archived	16.000
SMTP messages original size (bytes)	10,432.000
SMTP messages processed	8.000
SMTP messages unable to archive	0.000

What To Monitor if SMTP Archiving Task is not Processing Items

If the SMTP Server is receiving emails but the SMTP Task is not processing, then the 'Enterprise Vault SMTP Service' and 'Enterprise Vault SMTP Holding Folder' shows an increase in the "SMTP messages received" and 'Disk space % used' counts respectively. However, the count of "SMTP messages archived" in the 'Enterprise Vault SMTP Archiving Task' does not change. This behavior is expected if the SMTP Server is not started.

The event viewer and error log is the first point of call to troubleshoot any issue. The sample texts that appears in the error report log is mentioned the SMTP Task Error Log section. Additionally, administrators can enable dtrace on the "EVSMTPTASK" object in verbose mode to look for the exact root cause of the issue.

Storage Queue and Archives

The SMTP archiving task uses the EV CM APIs for ingestion. The first step is to store eml in storage queue. The storage queue acts as a staging area before the eml is finally stored in the archive.

The default name of the storage queue folder is 'EVStorageQueue' and there is one storage queue per storage server. The default location of this folder is under 'EV cache' folder. Storage Queue folder will be configured with the same security DACLs as any NTFS EV partition SYSTEM.

Multiple eml's can be written to a single 'Storage Queue Batch Stream' file based on size. This is done in order to reduce the overhead of writing each eml as a separate file.

The storage archive process will pick each 'Storage Queue Batch Stream' file and ingests into the vault store partition folder, with extension of .dvs file.

When 'Storage Safety Copy' is OFF, the copy of eml in the storage queue is removed immediate after it has been ingested into the vault store partition.

When Storage Safety Copy' is ON, the eml in the storage queue is preserved even after it has been ingested to the vault store partition. File will be removed from the storage queue after the ingested file on the partition has been backed up.

Tracking Enhancements in Enterprise Vault 12.2

With the Introduction of a Message Tracking Log, customers now have logging capabilities similar to Exchange. The Message Tracking Log may be used for Message Forensics, Mail Flow Analysis, Reporting and Troubleshooting.

When an Enterprise Vault SMTP server receives a message:

1. The service checks to see if Message Tracking is enabled.
2. If enabled, the service records message attributes to the tracking log in the specified location

Tracking logs are stored in the EV **Reports** folder by default in CSV format.

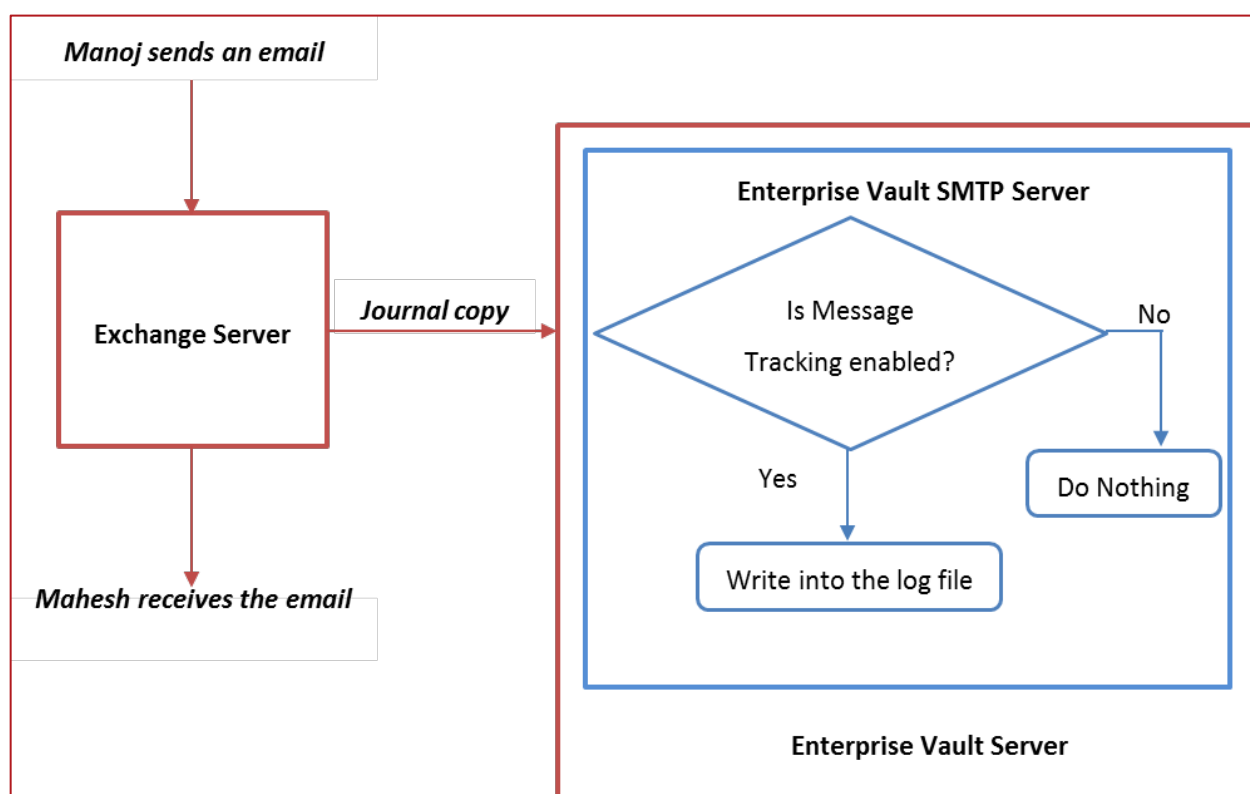


Figure 27 – Message Tracking Architecture

The SMTP Message Tracking feature is installed automatically during an upgrade or fresh installation of Enterprise Vault 12.2, and is disabled by default.

To enable message tracking, go to Vault Administration Console > Directory > site_name > Targets > SMTP > SMTP Properties. The Message Tracking tab is shown below.

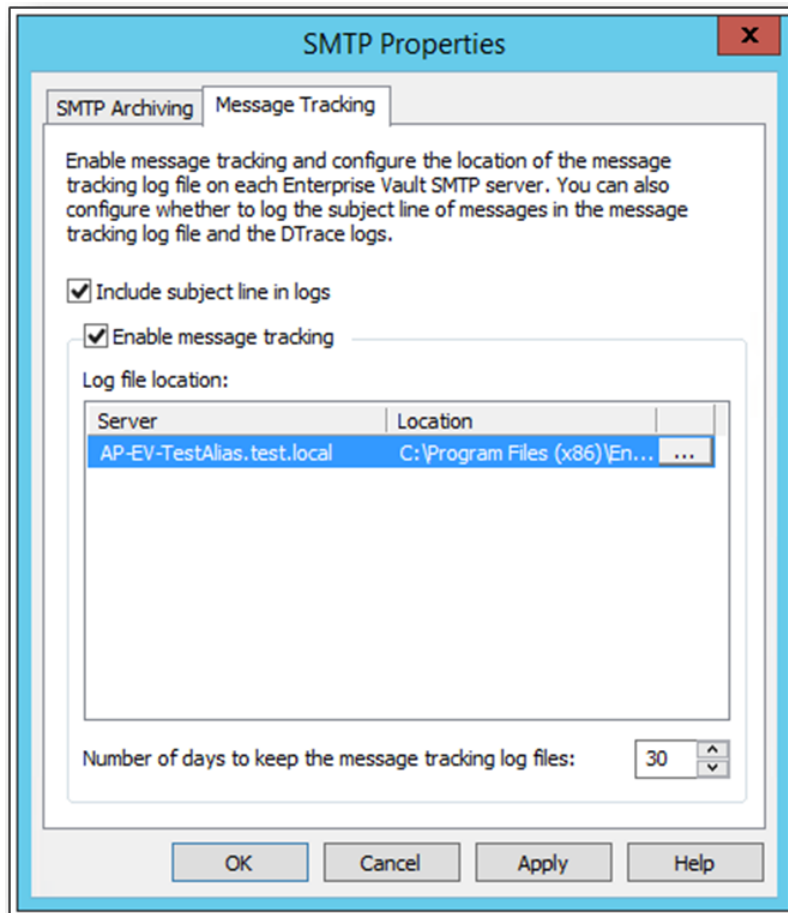


Figure 28 – Message Tracking settings in the Vault Administration Console

Include subject line in logs: Mark the checkbox to include subject lines

Enable message tracking: Mark the checkbox to enable

Log file location: If required, change the log file location for every EV SMTP server

Number of days to keep the message tracking log files: Specify how many days to keep the logs.

The following table breaks down the structure of each row in the log:

unid	qid	msgid	Subject*	mta	size	sender	submit-time
WFpS2ABjDJ8B	msg.00000-0	<de324ec4-275b-4770-9627-9ee80bd59914@journal.repor t.generator>	Test	as-exch15.moto.local	12916	rjones@moto.local	2016-12-21-15.30.56

*If “Include subject line in logs” is not enabled, this field will be blank.

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.

Copyright © 2020 Veritas Corporation. All rights reserved.

All rights reserved. Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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.

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