Enterprise Vault Whitepaper

Configuring Exchange archiving with minimal permissions

This document covers the minimal permissions required for Enterprise Vault in order to successfully achieve mailbox, journal and public folder archiving from Microsoft Exchange.

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

This document applies to the following version(s) of Enterprise Vault: 9.0, 10.0

This document applies to the following version(s) of Microsoft Exchange Server: 2003, 2007, 2010 and 2013.

Refer to Enterprise Vault Compatibility Charts for specific service pack releases of Microsoft Exchange that are supported by each Enterprise Vault version.

Document Control

Contributors

Who	Contribution
Karl Woodrow, EV Engineering	Technical content
Andy Joyce, EV TFE	Editor
Dan Strydom, EV TFE	Updates for Exchange 2013

Revision History

Version	Date	Changes
1.0	March 2012	Initial release
2.0	July 2013	Updated for Exchange 2013

Related Documents

Version	Date	Title

Table of Contents

Purpose of this document

In order to provision Microsoft Exchange target mailboxes and public folders for archiving, the Enterprise Vault archiving and provisioning tasks require permission to access and write to those mailboxes, as well as permissions to access specific other parts of the Exchange hierarchy in order to be able to enumerate the mailboxes available. The standard Enterprise Vault *Installing and Configuring* manual supplied with the software details the procedure required to grant the Vault Service Account a set of permissions at a higher level in the Exchange hierarchy that will although Enterprise Vault to access all mailboxes and public folders below that point. However, some Exchange administrators to implement Enterprise Vault using a more restrictive set of permissions, applied at lower levels in the hierarchy. This document details how to do that.

Intended audience

It is assumed the reader understands how to set Exchange permissions and understands the Exchange archiving functionality and architecture of Enterprise Vault.

When minimal permissions can be used

The *SetEVExchangePermissions.ps1* script, supplied with Enterprise Vault, is intended to apply permissions that ensure all Enterprise Vault functionality works without the need for additional configuration when new Exchange servers or databases are added into the Exchange organization.

In some circumstances it is possible to set the permissions at lower levels than detailed in the Enterprise Vault *Installing and Configuring* guide, and by the provided script *SetEVExchangePermissions.ps1.*

It is assumed that manual configuration of targets is to be completed. If the *Getting Started Wizard* is to be used instead then this requires a broader set of read permissions in order to automatically locate various objects (for example journal mailboxes) and therefore the minimal permissions approach detailed in this document **cannot be used.**

The minimal permissions must be applied manually using either AdsiEdit.msc or via the Exchange PowerShell command Add-ADPermission. When applying the permissions take care to note the required inheritance otherwise Enterprise Vault will not function correctly.

Minimal permissions required on information store objects

The following permissions are required on the information store objects (mailbox databases/public folder databases). These allow Enterprise Vault to access mailboxes and public folders. Applying these permissions at the lowest level in the Exchange hierarchy in Active Directory is discussed later.

Permission	Reason
Read (ReadProperty, GenericExecute)	Allows Enterprise Vault to read additional properties from information store objects. This enables more informative error information when checking task configuration. *For Exchange 2010 this permission is granted to Everyone by default (onto descendant mailbox and public information stores). Symantec recommend setting this permission to ensure in locked down Exchange deployments the archiving tasks continue to function correctly.*
Receive As (Receive-As)	Allows the task to connect and open any mailbox/public folder.
Administer Information Store (ms-Exch-Store-Admin)	Allows the task to connect and open any mailbox/public folder. Additionally by using administrative permissions Exchange uses less resource when performing permission checks when opening mailboxes.
Create named properties on information store (ms-Exch-Store-Create-Named-Properties)	Allows the tasks to create named properties. *The default Exchange permissions grant Everyone this permission by default. Symantec recommend setting this permission to ensure in locked down Exchange deployments the archiving tasks continue to function correctly.*
View Information Store Status (ms-Exch-Store-Visible)	Allows the task to bypass the default MAPI session limit (32) on the target Exchange server. Does not apply to Exchange 2013.

Where possible all permissions must be set to inherit to lower objects. For example when using AdsiEdit.msc for Windows 2003 you would need to select the 'Advanced' permission tab and ensure Apply onto is set to 'This object and all child objects'. For Windows 2008 the setting is 'Apply to:' with value 'This object and all descendant objects'. If using Add-ADPermission set -InheritanceType All.

Where to apply minimal permissions

Exchange 2003

Permissions required by VSA or task account (for mailbox, journal and public folder archiving and provisioning)	• Read • Receive as • Administer information store • Create named properties in information store • View Information Store Status
Recommended lowest level in Exchange hierarchy to apply these permissions	Set on each individual Exchange Server object with inheritance down to lower levels
Additional permissions required for provisioning task	None in addition to those specified above for archiving

Exchange 2007

Permissions required by VSA or task account (for mailbox, journal and public folder archiving and provisioning)	• Read • Receive as • Administer information store • Create named properties in information store • View Information Store Status
Recommended lowest level in Exchange hierarchy to apply these permissions	Set on each individual Exchange Server object with inheritance down to lower levels
Alternative lowest level to apply permissions	Permissions can be applied on specific databases or storage groups. However • for mailbox archiving, mailboxes in databases that don't have the required permissions should be excluded from provisioning or the archive task will log errors each time it runs • for public folder archiving, the mailbox database of the task's system mailbox and the public folder database must have the required permissions • read permission must be granted at least the server level (otherwise the archiving task cannot be configured)
Additional permissions required for provisioning task	In addition to permissions required for archiving, the VSA or task account requires access to managed folder content settings. The synchronization can be disabled by following the following articles: **http://www.symantec.com/docs/TECH126862** **http://www.symantec.com/docs/HOWTO57173**

Exchange 2010

Permissions required by VSA or task account (for mailbox, journal and public folder archiving and provisioning)	• Read • Receive as • Administer information store • Create named properties in information store • View Information Store Status
Recommended lowest level in Exchange hierarchy to apply these permissions	Set on each individual Exchange *database* object with inheritance down to lower levels. • For mailbox archiving, mailboxes in databases that don't have the required permissions should be excluded from provisioning or the archive task will log errors each time it runs • For public folder archiving, the mailbox database of the task's system mailbox and the public folder database must have the required permissions
Additional permission required for Exchange 2010	The archiving tasks require Read permissions to the Global Settings container
Additional permissions required for provisioning task	In addition to permissions required for archiving, the VSA or task account requires access to managed folder content settings. The synchronization can be disabled by following the following articles: **http://www.symantec.com/docs/TECH126862** **http://www.symantec.com/docs/HOWTO57173**

Exchange 2013

Permissions required by VSA or task account (for mailbox, journal and public folder archiving and provisioning)	• Read • Receive as • Administer information store • Create named properties in information store
Recommended lowest level in Exchange hierarchy to apply these permissions	Set on each individual Exchange *database* object with inheritance down to lower levels. • For mailbox archiving, mailboxes in databases that don't have the required permissions should be excluded from provisioning or the archive task will log errors each time it runs • For public folder archiving, the mailbox database of the task's system mailbox and the public folder database must have the required permissions

Additional permission required for Exchange 2013	The archiving tasks require Read permissions to the Global Settings container
Additional permissions required for provisioning task	In addition to permissions required for archiving, the VSA or task account requires access to managed folder content settings. The synchronization can be disabled by following the following articles: **http://www.symantec.com/docs/TECH126862** **http://www.symantec.com/docs/HOWTO57173**

About Symantec:

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

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

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

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