Best Practices: Protecting Exchange Server 2010 with Retrospect

Description:	This document outlines best practices for protecting a Microsoft Exchange Server 2010 environment with Retrospect.
Area of Protection:	Microsoft Exchange Server 2010
Retrospect Edition(s):	Retrospect 8 Multi Server (Part #: APPNEWMSV080EC) Retrospect 8 Single Server (Part #: APPNEWSSV080EC) Retrospect 8 Small Business Server (Part #: APPNEWSBP080EC – includes Exchange Agent) Retrospect 8 Disk-to-Disk (Part #: APPNEWDTD080EC)
Retrospect Add-On(s):	Retrospect Microsoft Exchange Agent (Part #: OPTNEWEXH080EC)
Use Case:	Sites needing to protect Microsoft Exchange Server 2010, whether in a standalone or clustered "database availability group" (DAG) configuration

Introduction

With Exchange Server 2010, Microsoft introduced several improvements related to backup, restore, and disaster recovery, including database availability groups, the Recoverable Items Folder, and support for long-term data storage. These new features provide disaster *prevention* capabilities that should be incorporated into Exchange backup and recovery plans whenever possible. This Best Practices document has been compiled to support you in getting the most out of the Retrospect Microsoft Exchange Agent add-on by leveraging the new capabilities in Exchange Server 2010 to complement Retrospect's data protection capabilities.

Configuring Exchange Server 2010 for Data Loss Prevention

When considering an overall data protection strategy, *prevention* methods should be considered before *recovery* methods. A good example is implementing RAID to *avoid* data loss due to hardware failure. This also holds true with planning for an Exchange environment, and Exchange Server 2010 includes several prevention methods worth implementing.

Employ database availability groups for high availability and database recoverability

Take advantage of Exchange Server 2010's database availability group (DAG) functionality, which provides automatic failover, mailbox redundancy, and even protection against the loss of an entire site by allowing two or more Exchange Servers to serve as a cluster,. What makes DAGs so worthwhile is their ease of setup and use. With previous versions of Exchange, one had to tackle the complicated task of setting up and managing a cluster separately. Exchange 2010 takes care of all the clustering setup and management under the hood, making setup and operation trivial.

The downside of DAGs is higher cost of entry, since a DAG's automated cluster failover requires Windows Server 2008 Enterprise Edition. However, the additional protection it offers makes good sense. For additional information on database availability groups, see:
http://technet.microsoft.com/en-us/library/dd979799(v=exchg.141).aspx.

Use retention policies and archiving as defense against accidental item deletion

Exchange Server 2010 includes several methods for increasing recoverability of accidentally deleted mailbox items. By configuring these settings for maximum protection, you can ensure that end-users will be able to recover items when needed..

Retention policies and tags:

Exchange Serer 2010 makes it easy to assign retention policies to mailbox folders (such as the Deleted Items folder) and to assign different policies to different groups of users. For example, a retention tag could specify that, upon the Deleted Items folder being emptied, its contents are to be moved to the Recoverable Items folder. A retention policy for a group of users could then combine that tag with one that later moves items from the Recoverable Items folder in those users' mailboxes to the Recoverable Items folder in the users' personal or cloud archive mailbox. For additional information on retention policies and tags, see: http://technet.microsoft.com/en-us/library/dd297955(v=exchg.141).aspx.

Archiving

Exchange Server 2010 supports the creation of personal (local) and cloud (Office 365) archives. Archive mailboxes duplicate the structure of each user's primary mailbox, and users are able to access them seamlessly with Outlook 2007 and later and the Outlook Web App. With Exchange Server 2010 SP1 and later, archive mailboxes can be stored in a separate mailbox database, or even on a separate Exchange Server, which allows archived email to be stored on less expensive storage. The default quota of 50 GB per mailbox allows for a generous archive. For additional information on archiving, see: http://technet.microsoft.com/en-us/library/dd979800(v=exchg.141).aspx.

Configuring Exchange Server 2010 for Retrospect Backups

To achieve the best results, it's necessary to install additional Microsoft components and configure certain settings in Exchange Server.

- *Microsoft .NET Framework 4.x* – Version 4 of the .NET framework can be installed alongside .NET 3.5, which is required by Exchange Server 2010. Version 4 is required for Retrospect to bridge to the Exchange Management Shell. http://www.microsoft.com/en-us/download/details.aspx?id=24872
- *Microsoft Exchange MAPI and CDO 1.2.1* – The Microsoft Exchange Server MAPI Client and Collaboration Data Objects are necessary, especially if you'll be backing up mailboxes with Retrospect. http://www.microsoft.com/en-us/download/details.aspx?id=1004
- *Client Access Server Role* – Ensure that the Client Access server role is activated and configured on the same Exchange Server as the Mailbox role.
- *Activate Outlook 2003 Support* – This setting needs to be configured during setup to allow Retrospect access to mailboxes, even if your organization does not have clients using Outlook 2003. (Note: If you completed Exchange setup without activating Outlook 2003 support, adding a Public Folder database will have the same effect.)
- *Disable Circular Logging* – Though disabled by default on Exchange Server 2010, this setting should be verified by the administrator to support differential and incremental/log backups.
- *AVOID PowerShell 3* – PowerShell 3 is incompatible with Exchange Server 2010 cmdlets.

Configuring Retrospect for Exchange Server 2010 Backup

The following tips will ensure a smooth setup process. For additional information, please refer to *Appendix B – Exchange Server Agent* starting on page 359 of the Retrospect User's Guide.

Configuration Tips

- Choose to install either the Retrospect Client or application on your Exchange Server. It's most common to install the client, as it has the least amount of impact on server performance.
- For an Exchange Server VM, install the Retrospect Client software in the guest OS to allow Retrospect to properly access the Exchange Server's mailbox databases.

- If it does not already exist, create a Retrospect Backup User (RBU) account in Active Directory and ensure that it has been added to the following groups: Domain Users, Domain Administrators, Backup Operators, Organization Management, and Exchange Trusted Subsystems. If the Retrospect application has been installed directly on the Exchange Server, you will also need to add the RBU account to the Local Admins group.
- Retrospect must to run as the RBU account (verify in Configure > Preferences > Security).
- Ensure that a Retrospect Exchange Server Agent license code has been added to the Retrospect server's License Manager. If you will be protecting Exchange Servers in a DAG, one Exchange Agent license is required for each Exchange Server that Retrospect will access. (Note: Retrospect 8 Small Business Server edition includes an Exchange Agent license.)
- Assign the Exchange Agent license(s) to the Exchange Server(s) in Configure > Volumes by clicking on an Exchange Server under My Computer (if the Retrospect application has been installed directly on the Exchange Server) or Backup Clients (if the Retrospect Client software is installed on the Exchange Server). Retrospect will ask your permission to assign a license, ask for the RBU login credentials if you're assigning a license to an Exchange Server running the Retrospect Client, and then it will populate the list of databases and mailboxes.

Backup Tips
- Be aware of the differences in backup types: Unlike Retrospect's Smart Incremental backups of the file system, which ensure that each destination Backup Set is given one copy of all the files needed for a complete restore, Exchange Server backups can only use the more traditional Full, Differential, and Incremental (also called Log) backup methods. This means it's possible to end up with a Full backup on one Retrospect Backup Set and the Log backup on a completely different Backup Set. In such a case, you'd need both Backup Sets to perform a complete restore of the Exchange Server mailbox database(s). Retrospect tracks the location of Exchange Server backups in the Database Backup History window.
- Consider using separate Backup Sets for Exchange Server backups: Though this is not a requirement, it's often easier to manage Exchange Server backups when they're confined to their own Backup Sets. Doing so will also offer the best performance for backups and restores.
- Perform regular Full backups: The greater the number of Exchange log files present from Incremental/Log backups, the longer it will take to restore those files, and the longer it will take the Exchange Server to replay those changes and bring the mailbox database(s) current. Performing regular Full backups will ensure the best restore performance.
- Back up your Active Directory server: It's important to back up Active Directory servers on a regular basis. This is especially true when Exchange Server 2010 is present, for all the data that's shared between the two. (Note: If both the AD and Exchange Servers must be recovered, restore the AD server first; that will make Exchange Server recovery faster.)

Restore Tips
- Implement a DAG: Employing a database availability group provides outstanding high availability and mailbox resiliency with automated failover and database/mailbox replication. When restoring to a DAG member server, Retrospect will only restore to an active node.
- Implement supportive retention and archive policies: Doing so will reduce demands on the backup administrator by allowing users to self-serve recovery from within Outlook.
- Test restores using Exchange Server 2010's recovery database: Creating a recovery database will allow you to perform test restores to your Exchange Server without needing to take an mailbox databases offline. For information on Exchange Server 2010's recovery database, see: http://technet.microsoft.com/en-us/library/dd876954(v=exchg.141).aspx.