Revision: This manual has been updated for Version 7.5 (March 2015).
Software Version: 7.50

© 2015 EVault Inc.

EVault, A Seagate Company, makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, EVault reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of EVault to notify any person of such revision of changes. All companies, names and data used in examples herein are fictitious unless otherwise noted.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval System or translated into any language including computer language, in any form or by any means electronic, mechanic, magnetic, optical, chemical or otherwise without prior written permission of:

EVault, A Seagate Company
c/o Corporation Trust Center
1209 Orange Street
Wilmington, New Castle
Delaware 19801
www.evault.com

EVault, EVault Software, EVault SaaS, and EVault DeltaPro, are registered trademarks of EVault Inc. All other products or company names mentioned in this document are trademarks or registered trademarks of their respective owners.

Acknowledgements: Two encryption methods, DES and TripleDES, include cryptographic software written by Eric Young. The Windows versions of these algorithms also include software written by Tim Hudson. Bruce Schneier designed Blowfish encryption.

"Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright 2001-2006 Robert A. van Engelen, Genivia Inc. All Rights Reserved. THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

The EVault Software Agent, EVault Software CentralControl, and EVault Software Director applications have the encryption option of AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced "Rain Doll") was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm was chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the new Federal Information Processing Standard (FIPS).

The EVault Software Agents and EVault Software Director applications also have the added security feature of an over the wire encryption method.
# Contents

1 **Exchange Plug-in Overview** .............................................................................................................. 3  
1.1 Additional Documentation ................................................................................................................ 3  

2 **Installing the Exchange Plug-in** .................................................................................................... 4  
2.1 Cluster Support ................................................................................................................................ 4  
2.1.1 Exchange 2007 CCR (Cluster Continuous Replication) DR Support ........................................... 4  
2.1.2 Exchange 2010/2013 DAG (Database Availability Group) DR Support .................................... 4  
2.2 Licensing .......................................................................................................................................... 4  

3 **Backing Up Exchange Databases** .................................................................................................... 5  
3.1 Creating an Exchange Server Backup Job ....................................................................................... 6  
3.2 Backup Types ..................................................................................................................................... 7  
3.3 Exchange 2007 ................................................................................................................................ 7  
3.4 Exchange 2010/2013 ......................................................................................................................... 7  
3.5 Backup Options .................................................................................................................................. 8  
3.6 PowerShell Log Messages ................................................................................................................. 10  
3.7 Scheduling your Exchange Backup .................................................................................................. 11  
3.8 Remaining Steps for Job Creation ..................................................................................................... 11  
3.9 Verifying Your Backup ...................................................................................................................... 12  
3.10 Optimizing Exchange Backups ........................................................................................................ 12  
3.10.1 Choosing a Backup Schedule ...................................................................................................... 13  
3.10.2 How Exchange Maintenance Affects your Backups ................................................................. 16  
3.10.3 How Exchange Backups Affect your Maintenance ................................................................. 16  

4 **Restoring Databases** ....................................................................................................................... 18  
4.1 About Disaster Recovery (DR) ......................................................................................................... 18  
4.2 Recovering from a Worst Case Disaster .......................................................................................... 19  
4.3 Restoring the Exchange Data ......................................................................................................... 19  
4.3.1 Exchange 2007 ............................................................................................................................ 19  
4.3.2 Exchange 2010/2013 ................................................................................................................ 20  
4.4 Restoring a Standalone Database .................................................................................................... 21  
4.5 Restoring a DAG Replica Database .................................................................................................. 22  
4.6 Storage Group and Database Selection for Restore ....................................................................... 22  
4.6.1 Exchange 2007 ............................................................................................................................ 22  
4.6.2 Exchange 2010/2013 ................................................................................................................ 24  
4.7 Storage Group and DB Selection for Restore Destination ............................................................. 25  
4.7.1 Exchange 2007 Restore Destination .......................................................................................... 25
4.7.2 Exchange 2010/2013 Restore Destination .................................................. 26
4.8 Troubleshooting – Restore to an Alternate Location ........................................... 27

5 Granular Restore for Microsoft Exchange – Sharing DR Safesets .................................. 28
  5.1 Sharing a DR Safeset for Granular Restore with Windows CentralControl .............. 28
  5.2 Sharing a DR Safeset for Granular Restore with Web CentralControl ..................... 29

6 Appendix ....................................................................................................................... 30
  6.1 Backup Considerations for Exchange 2007 CCR and LCR Setups .............................. 30
    6.1.1 Disaster protection for LCR ............................................................................. 30
    6.1.2 Exchange 2010/2013 Database Availability Group (DAG) ............................... 30
    6.1.3 Restore Considerations .................................................................................. 31
1 Exchange Plug-in Overview

This guide describes how to back up and restore Microsoft Exchange databases using the Exchange Plug-in.

This guide also describes how to share a DR backup safeset so you can restore specific mailboxes, messages or other objects to a .pst file using the Granular Restore for Microsoft Exchange application.

Note: Support has ended for Exchange MAPI jobs. You must delete any jobs with this legacy type from the Agent before you can upgrade the Agent. If you upgrade an Agent where a legacy Exchange MAPI plug-in is installed, the plug-in will be removed. To restore from legacy Exchange MAPI jobs on the vault, install a version 7.34 or earlier Agent with the Exchange MAPI Plug-in, and use the Restore from another computer procedure.

1.1 Additional Documentation

The “Agent for Microsoft Windows User’s Guide” has information on installation of the Agent and Plug-ins, and Agent configuration.

For information about managing Exchange backups using Portal, see the Portal online help.

The online help for Web CentralControl and Windows CentralControl has information about managing Exchange backups using these legacy interfaces.

See the latest Windows Agent release notes (32-bit or 64-bit) for a list of supported platforms.
2 Installing the Exchange Plug-in

The Exchange Plug-in is installed during the Windows Agent 64-bit installation. The Plug-in can be installed when installing the Agent or it can be installed later, by re-running the installation with the Modify selection. The Cluster Support Plug-in can be installed the same way.

**Note:** Support has ended for Exchange MAPI jobs. You must delete any jobs with this legacy type from the Agent before you can upgrade the Agent. If you upgrade an Agent where a legacy Exchange MAPI plug-in is installed, the plug-in will be removed. To restore from legacy Exchange MAPI jobs on the vault, install a version 7.34 or earlier Agent with the Exchange MAPI Plug-in, and use the *Restore from another computer* procedure.

For more information, see the Windows Agent guide.

2.1 Cluster Support

Clustering is supported for Windows Agents, with a separately licensed Cluster Support Plug-in. The main function of the Cluster Support Plug-in is for the Agent on an Exchange Server, which has a virtual IP address in the cluster, to be able to follow the server when it fails over to another node in a cluster.

The Agent can still access its configuration (on a shared drive), and scheduled backups will occur as usual, without it looking like a "different" backup and causing a reseed.

2.1.1 Exchange 2007 CCR (Cluster Continuous Replication) DR Support

DR on CCR:

- Agent, Cluster Plug-in and Exchange DR Plug-in.
- Shared resource required to handle failover and function with the Cluster Plug-in.

2.1.2 Exchange 2010/2013 DAG (Database Availability Group) DR Support

- The DAG requires failover clustering to be installed in a Majority node configuration, which does not require any shared drives.
- See the Agent User Guide for information about installing and using the Cluster Support Plug-in.

2.2 Licensing

The Exchange Plug-in requires a separate license. The license will be automatically supplied from the vault.

See the Agent User Guide or the CentralControl Guide for more information on licensing.
3 Backing Up Exchange Databases

To back up your Exchange Server you will first need to add a new Agent, create a new job, and then schedule that job to run. The first backup of an Exchange database is forced to be a “seed” backup, even if “incremental” is selected. Future backups default to the setting on the job.

Backup terms that apply to the Exchange Plug-in:

- **Seed**: The “first” backup that is performed is referred to as a seed, and is a complete backup of selected Exchange database. However, a seed is not a selectable type of backup. The seed is created automatically as your “first” backup whether Incremental or Full is selected as the backup type. The seed usually takes the greatest amount of time to complete.

- **Full**: Full refers to how it performs its Full backup type. This reads all the information on an Exchange Server. The backup type Full, using a Delta (changed data) technique, backs up and optimizes all the changes in your Exchange (.edb, .log, etc.) that have occurred since the last backup. This data is added to the original safeset to complete the entire backup safeset. Using Full with the Delta technique saves a great deal of time, as only changes are transmitted to the Vault. It is recommended to periodically schedule a full backup as this will reduce the size of the log files, which in turn will reduce the time required for a recovery if needed.

- **Incremental**: Incremental backups are transaction logs and the checkpoint file only. To produce a complete picture of the up-to-date Exchange database the incremental transaction logs are added to the safeset. Incremental backups take the least amount of time to perform. During recovery, the log files will be played back to achieve the most up to date restore since the last backup.

**Note**: When backing up an Exchange database, do not use Open Transaction Manager™ or Open File Manager™. The backup does not benefit from OTM or OFM in this case. Also, using OTM or OFM may slow the backup.

- All Exchange services remain operational while backups occur.
- Always perform a Full backup after database maintenance or recovery.
- Always perform ‘full system backup (including a system state backup)’ plus a ‘full Exchange backup’ every time you install new hardware/software. Having these backups will significantly simplify bare-metal recoveries.
- When an Exchange server has multiple Storage Groups (Exchange 2007) or Databases (Exchange 2010/2013), you can put the different Storage Groups/Databases into separate jobs. The jobs may then be run simultaneously.

**Note**: Do not create parallel jobs for the same Storage Group (Exchange 2007) or Database (Exchange 2010/2013). This combination can result in conflicts that will prevent the jobs from completing successfully. This also applies to jobs created by Third Party backup applications or Agents on other DAG members.

**Note**: This guide provides instructions for performing tasks using legacy CentralControl applications. For instructions using Portal, see the Portal online help.
3.1 Creating an Exchange Server Backup Job

1. Launch the New Job Wizard. Set the Backup type, select a vault profile and enter a Job Name, as described in the CentralControl manual, “Create a Job”. The following selections will appear in the Backup source type menu.

2. On the New Job Wizard - Backup Source Type window, select the appropriate Exchange DR from the menu, and then click Next.

3. The Encoding type is Unicode, so some database names might not display properly in selection screens. You can back these databases up, though. Click Next to continue.

4. Select a Destination for the backup. Click Next.

5. Enter a name for your job. Enter a job description (optional). Click Next.

6. On the Source screen, click Add to open the Include/Exclude dialog.

7. Information about the Exchange server will appear. Expand the entry to display its contents.

8. Select databases or components to back up, and click Include. The items that you choose will appear in the lower pane of the screen.

9. Click OK to continue.

10. Click the Options button to open the Server Backup Options panel.

11. Select the Incremental backup type. The first backup will always be a Full “seed” of the Exchange database regardless of the whether Incremental or Full is selected. Subsequent to the first backup, only the transaction log files will be backed up when is Incremental selected. The default backup type is Incremental.

   Note: Incremental backups for Exchange cannot be deferred, even if deferring is enabled for the job. Deferring can be applied to full backups for Exchange.

12. Select the Delete Exchange log files after backup checkbox if you want to instruct the Exchange server to delete the log files that you have just backed up. This option helps to conserve space on your Exchange server, and reduces the time required for the next backup. Deselect this option if you want to maintain the original Exchange logs for other specific purposes.
13. Click Next to proceed to the next step in the New Job Wizard. Complete the job as you normally would, and then click Finish.

   *Note:* You can edit your Exchange backup options by opening the Job Properties panel of a selected job and clicking on the Source tab.

### 3.2 Backup Types

The Exchange Plug-in offers two methods for backing up Exchange: Full and Transaction Log (Incremental). When the Full option is selected, the Plug-in will back up the transaction log and database files for the Storage Group(s) (Exchange 2007) or Database(s) (Exchange 2010/2013) selected.

When the Incremental option is selected, the Plug-in will back up the transaction log for the Storage Groups/Databases selected. You must have done a FULL backup before this.

With any successful backup of Exchange, the transaction logs for the selected Storage Groups/Databases are truncated.

### 3.3 Exchange 2007

If you are running a Windows Agent 64-bit (version 6.5 or higher) on an Exchange 2007 Server, and have installed the Exchange Plug-in, you will see an option in Backup Source Type called Exchange 2007 DR.

This is applicable to new jobs only. If you have existing DR type Exchange backups, they will remain as DR type Jobs.

There are three types of replication strategies in Exchange 2007:

- CCR (Cluster Continuous Replication) that replicates to another Exchange Server and has failover capabilities
- LCR (Local Continuous Replication) that replicates locally
- SCR (Standby Continuous Replication) that also replicates to another Exchange server but does not have failover capability

   *Note:* For a Backup to work on Exchange 2007 CCR (Cluster Continuous Replication), you must have only one database per Storage Group. Typically, you would use one backup job for each Storage Group.

### 3.4 Exchange 2010/2013

There are a number of changes in Exchange 2010/2013 that affect replication strategies:

- CCR, LCR and SCR are no longer used to replicate the Exchange Data and provide failover capabilities
- DAG (Database Availability Groups), which replicates the database to other Exchange Servers and has failover capabilities

Storage Groups are no longer used, each database has its own checkpoint file and set of transaction logs.
To backup the replica or copy databases in the DAG, Exchange 2010/2013 uses the Exchange Replica VSS Writer which is connected to the Microsoft Exchange Replication Service. This VSS Writer can only backup the databases; restore is not supported.

**Note:** Only databases that are in a Mounted or Healthy state are backed up. Any unmounted databases will be skipped. If the skipped database(s) are in a Mounted or Healthy state for the next backup (in the case of a subsequent incremental backup), they will not need to be reseeded. If all of the selected databases are unmounted, or not in a Healthy state, the job will fail.

### 3.5 Backup Options

There are three options available to the user when the Exchange Plug-in is performing a backup. Exchange 2010/2013 do not use the ‘Only Back Up Active Instance’ option.

**Backup Type**

The Exchange Plug-in supports both Full and Incremental (or Transaction Log) backups.

When performing a FULL, the Plug-in will back up the databases, checkpoint file and transaction logs for the selected Storage Group(s) in Exchange 2007 or Database(s) in Exchange 2010/2013. When performing an INCREMENTAL, the Plug-in will backup only the transaction logs and checkpoint file for the selected Storage Group(s) or Database(s). By default, the backup type will be FULL.

Traditionally, an Incremental backup would only contain the checkpoint file and transaction log files for the Storage Groups or Database(s) selected. With this Plug-in, the transaction logs will be rolled up with the contents of the previous FULL and Incremental backups. This simplifies the restore process from an Incremental because it can be done from a single safset.

An Incremental backup requires that at least one FULL backup has been run previously. The FULL backup establishes a baseline for all subsequent Incremental backups.

If the Plug-in determines that it is unable to run an Incremental backup, it ignores the option and runs a FULL backup instead. This does not occur when validation has failed or there were changes to the log files since the last incremental backup. In those cases the backup will fail.

It is possible to select Incremental Backups for both scheduled and ad-hoc backups.

**Note:** Incremental backups for Exchange cannot be deferred, even if deferring is enabled for the job. Deferring can be applied to full backups for Exchange.

**Validate Exchange Database**

When backing up Exchange the integrity of the Exchange Database files is not validated. When selected, the Plug-in will use a utility provided by Exchange to validate the exchange data during the backup. By default, this option is enabled.

The validation runs in parallel with the backup to validate transaction logs and database files. If it detects an error, the Agent reports the corruption and fails the entire backup.

The Exchange Plug-in provides an option to validate the integrity of the databases and transaction log files during the backup. The validation option is offered as a job setting as well as a scheduled option.
Only Backup Active Instance

Exchange 2007 allows backups to be performed against a replica of the Exchange database(s) instead of the active copy.

This option really only applies to backups that are run on an LCR configuration. When enumerating the list of Storage Groups to be backed up, the Plug-in will determine whether the Storage Groups support Local Replication (LCR). If all selected Storage Groups support local replication, the Plug-in will use the replica copy for backup. If one or more Storage Groups do not support local replication, the Plug-in will use the active copy for backup. When this is option is turned on, the Plug-in will only use the active copy for backup. If the Exchange configuration does not support LCR, the option is just ignored. By default, this will be disabled.

Include/Exclude

Choose a Server or one or more Storage Groups/Databases.

Note: With CCR, in Exchange 2007, backups can only be performed at the Storage Group level. You cannot select an individual database for backup. However, you can restore a single database from a Storage Group.

With LCR and SCR, you can select more than one database for backup.
With Exchange 2010/2013 DR backups, you can select more than one database for backup in a single job:

![Exchange Plug-in 7.5 User Guide](image)

3.6 PowerShell Log Messages

The Agent with the Exchange Plug-in uses PowerShell to run commands. This can produce PowerShell-related Eventlog popup messages.

At backup time, you may see a warning message similar to this:

![Eventlog Service](image)

You will need to periodically clear the PowerShell Eventlog messages by following the instructions on this screen.
3.7 Scheduling your Exchange Backup

1. Select your Exchange Agent in the left pane of the CentralControl application. The Exchange job you created plus the Schedule, Global and Inventory files appear in the right pane.
2. Double-click the Schedule file. The Schedule List appears.
3. Click the New button. The Schedule wizard launches.
4. Work through the Schedule wizard as described in the CentralControl manual. “Add a New Schedule Entry.”
5. On the Schedule wizard – Options page, make sure Incremental backup is selected. This ensures that only your Exchange transaction logs are backed up.
6. On the Schedule wizard – Weekly page, select the days when you want the job to run (e.g. Monday through Friday).
7. Continue working through the Schedule wizard until finished.
8. Repeat the above procedure to run a backup of your Exchange job once per week with Full backup selected.
9. Next, you should decide how to tailor your backup and recovery options based on your specific Exchange server.

3.8 Remaining Steps for Job Creation

The Options screen

Quick file scanning: Enabling this option (where available) reduces the amount of data read during the backup process. Any file streams that are deemed unchanged since the last backup are skipped over. If this setting is disabled, files are read in their entirety.

Disable deferring: This option allows you to run the job without stopping, even if it means extending the run beyond the Backup time window.

Backup type: The first time you back up an Exchange database, it will be a backup type of Full. If you choose Incremental for your first backup, a Full backup will run instead. Subsequent backups can run as Incremental. (Remember that you should run a full DR backup at least once per week.)

2. Encryption: You can optionally use encryption. Select an Encryption type from the list.

Compose your own Password for encryption. This is not stored anywhere on the system. If you lose this password, your data will not be accessible.

3. Choose from the Log Options that follow. Log files are created on the server machine (with the Agent) in directories using the job names.

Create log file: Enable this option to generate log files for each job executed. These printable log files report start-connect-completion and disconnect times, file names (i.e., the name of each file that was copied during a backup process), and any processing errors.
Log detail level: You can select a detail level of None, Summary, Directories, or Files. Detailed logging creates large log files, but this is useful for troubleshooting problems.

Changing the Log detail level only affects log files that are created from that point on. It does not affect any previously created log files.

Automatically purge expired log files only: You can automatically purge expired log files, or keep a selected number of them before they get deleted. The oldest file is deleted first.

Keep the last <number of> log files: You can specify how many log files to keep. When that number is reached, the oldest log file will be deleted to make space for the new one.

4. Run the job immediately, Schedule the job, or Just exit from this wizard: You can run your job immediately, or schedule it for later. If you click Finish and simply exit, the job will still be available.

3.9 Verifying Your Backup

After a successful backup, you may check the safeset properties by right-clicking on the safeset, and choosing Properties (or using F2).

In the logs directory you can view the log file that the backup produced.

You may also have set the option to receive an email notification on a successful or failed backup. See the “CentralControl Operations Guide”.

3.10 Optimizing Exchange Backups

Optimizing your Exchange backups and restores requires creating a schedule of both regular Incremental backups and periodic Full backups.

A user should usually use the "Incremental" setting when setting up an Exchange backup type.

Optimizing the speed of your restore jobs requires a periodic "Full Backup", which backs up your Exchange server by first creating a full seed of the complete database. By default, all later backups are incremental and are transaction logs only. This means that only changes are transmitted to the vault. The transaction logs are added to the seed to produce a complete picture of the up-to-date Exchange database. Over time, transaction logs can accumulate, creating safesets with many log files. We recommend performing a "Full Backup" periodically. A Full Backup instructs the Agent to create a new delta of the complete Exchange database.

To optimize your Exchange backups and restores, we recommend you first create a backup job with the Incremental backup type. Schedule the job to run frequently (e.g. Monday through Saturday). Next, create a new schedule to periodically run the job with the Full backup type (e.g. Sunday only). If you are not sure how many transaction logs have been added to your safeset, open the job in CentralControl and check its backup log for the approximate number of files being backed up. If the "Log detail level" is set to Files, all Exchange transaction logs are listed together as .log files.

There might be other cases when you should consider forcing backup to "Full":

- A job fails and log and/or Windows Event Viewer - Applications indicates an error.
- You want to eliminate log files in the backup. This could save time on log replaying when restoring.
• You are performing database repair, defragmentation or recovery.
• You are updating the Exchange server to the latest Service Pack.

**Note:** Defragmentation of the database will cause the database to re-seed. The database is completely rebuilt during defragmentation so it is considered a new file.

In addition to the above, always check the job log for the progress of backup and the log and Windows Event Viewer > Applications for the progress of restore. Remember, that restore is a two step process - the first one ends when restore job ends and the second starts straight after that if you have selected the “Start Hard Recovery” option in the restore job. The progress of the first step is recorded in the log and the progress of the second is in Windows Event Viewer > Applications.

It is recommended NOT to run Full backups within your regularly scheduled Exchange maintenance time window. Your maintenance will be put on hold during a backup.

For all Exchange recovery strategies, please refer to Microsoft Exchange documentation.

The following pages illustrate how different backup schedules will affect your vault storage for various sizes of Exchange databases.

### 3.10.1 Choosing a Backup Schedule

The following three scenarios present three different Exchanges with different amounts of daily traffic and number of users. The recommended backup schedule differs based on the size of the Exchange database as well as your backup and communication needs.

* For Low Traffic / ~250 Users
* For Medium Traffic / ~1000 Users
* For High Traffic / ~4000 Users

The examples also show how the schedule can affect your safeset.

**Note:** Your actual results will vary depending on your traffic, database maintenance, and archive settings. **Note:** Logs are data, and are considered part of the total data transferred.
Low Traffic/250 Users

In this example, the Exchange Server has approximately 4GB of data and approximately 250MB of daily data traffic or 250 users. Notice that on the second week’s Saturday a Full backup is performed. All changes (delta) to the Exchange server are transferred to your safeset. The size of the safeset is reduced because the accumulated 2-week Logs approximate the 2 week’s changes, and have already been incorporated into your Exchange database.

Medium Traffic / 1000 Users

In this example, the Exchange Server has approximately 16GB of data and approximately 1GB of daily data traffic or 1000 users. Notice on Saturday a Full backup is performed. All changes (delta) to the Exchange server
are transferred to your safeset. The size of the safeset is reduced because the accumulated week’s logs approximate the week’s changes and have already been incorporated into your Exchange database.

**High Traffic / 4000 Users – Twice Weekly Full**

In this example, the Exchange Server has approximately 64GB of data and approximately 4GB of daily data traffic or 4000 users. Notice that on the mid-week Wednesday Full backup and on the Saturday Full backup, all the changes (delta) to the Exchange are transferred to your safeset. The size of the safeset is reduced because the accumulated 3-day logs approximate the changes over these 3 days and have already been incorporated into your Exchange database.

**High Traffic / 4000 Users – Once Weekly Full**

In the case of a High Traffic server, you might not want to use your communications bandwidth for backups during the mid-week period. In this case, you may prefer using the schedule outlined in this figure and perform a
Full backup on Saturday only. The speed of your bandwidth and your backup time window schedule may be determining factors. Also, a Saturday Full backup can defer onto Sunday if necessary.

3.10.2 How Exchange Maintenance Affects your Backups

Your regularly scheduled Exchange maintenance can affect how much data is transferred to your safeset during a Full backup. If, for example, you run daily maintenance on your Exchange server, then the database will be changing considerably each day. When performing a Full backup, these changes will be incorporated into your safeset. This will result in longer Full backup times, as you will be transferring more data. Your maintenance schedule will not affect an Incremental backup. In this case the transaction logs are the only data being transferred.

Note: Your backup has priority over the MDB (messaging database) maintenance schedule and as such will complete ahead of regular maintenance.

3.10.3 How Exchange Backups Affect your Maintenance

Your Full backup can also affect how your maintenance is performed as your backup jobs have priority over the MDB maintenance schedule. If your maintenance is run concurrently with a backup job, your maintenance will be put on hold until the backup completes.

If there is still time within the maintenance schedule window the maintenance can complete. If however, you ran Full backups every night during the time scheduled for maintenance, then it is possible that your Exchange would not have time to complete its maintenance. It is important to schedule your maintenance and Full backups so that they are not in conflict. Running an Incremental backup job will not significantly affect your maintenance schedule as only the transaction logs are being transferred.

This effect will also vary depending on the size and activity of your MDB as well as your maintenance schedule. Maintenance scheduling is done at the storage group level by default within Exchange but can be customized for each MDB.

The Exchange (MDB) maintenance schedule, effects, and defaults are detailed in Microsoft knowledge base article Q271222 at http://support.microsoft.com/. This article outlines performance costs and makes several recommendations.

The default maintenance schedule for Exchange is between 1:00 am and 5:00 am. Your regular maintenance performs three jobs:

- Checking Active directory for deleted mailboxes.
- Deleting any mailboxes or messages that are older than your set retentions.
- Defragmenting the MDB store while still online.

In the case of Exchange 2010/2013, online defragmentation is no longer only part of the database maintenance process. Online defragmentation can run in the background continuously when Enable background database maintenance (24x 7 ESE scanning) is selected. This setting is enabled by default.

As jobs 2 and 3 are disk-intensive jobs your maintenance should be scheduled outside of the time scheduled for a Full backup.
Running specific Exchange utilities such as ESEutil (extensible storage engine) require unmounting the MDB store. Backups cannot occur while running this utility. See Microsoft knowledge base article Q192185 at http://support.microsoft.com/
4 Restoring Databases

Restoring an Exchange Server (DR) is a two-step process. The first step in the process ends when the Restore job ends, and the second one starts right after that if you have selected the “Start Hard Recovery” option in the restore job. The progress of the first step is recorded in the restore log, and the progress of the second is recorded in Windows Event Viewer.

- For Exchange, you must unmount and set for “overwrite” (in the Exchange Management Console) the databases that you are restoring.

- For all Exchange recovery strategies, please refer to the Microsoft Exchange documentation on Microsoft’s website.

Restoring selected Exchange Mailboxes and Public folders only is a simpler process than restoring an entire Exchange Server (i.e., disaster recovery). For this, the Exchange Plug-in provides mailbox-level restore options.

Note: This guide provides instructions for performing tasks using legacy CentralControl applications. For instructions using Portal, see the Portal online help.

4.1 About Disaster Recovery (DR)

This section describes how to restore an Exchange server after a worst-case disaster.

With Exchange 2007, the introduction of multiple storage groups and databases adds complexity to restoring.

Exchange 2010/2013 have removed the use of storage groups, and allowed for the use of multiple databases, each having its own checkpoint file and set of transaction logs. This reduces some of the complexity for recovery work.

However, using the /disasterrecovery option allows you to run setup in Disaster Recovery (DR) mode to rebuild a server previously lost in case you have no full drive backups available for restore.

To fully recover from a total disaster, you need the following:

- Any replacement hardware, if necessary.

- The original operating system disks that were being used, including any applicable service packs or fixes.

- Full drive backups of the system drives, and other logical drives where critical applications or data were installed. A “Full backup” consists of the ‘System State backup’ and the ‘full drive or system backup’. A ‘System State backup’ for Windows Server captures Active Directory, registry, IIS metabase, and types of data that may not be backed up by some other backup systems.

- Exchange database backups.

- Along with backups of the information store database, you may also need backups of ancillary databases such as the SRS databases and KMS databases.

- All patches and settings previously applied.
4.2 Recovering from a Worst Case Disaster

Reconfigure hardware that is similar to the original hardware.

1. Create a logical drive that matches the original configuration. Although hardware does not always need to be identical, be aware that some drivers that are listed in the backup set may be incompatible with hardware on the new systems, and may require you to manually remove or install drivers in Safe mode. Test the system state recovery on replacement hardware before you actually need to perform a system state recovery.

2. Reinstall the operating system. Install the same version of Windows Server as a stand-alone server to the same drives and paths to which Windows Server was previously installed. Use the same server names as those used before.

3. Restore full-drive backups. The full backup consists of your ‘System State backup’ and the ‘full drive or system backup’. By restoring the system state, you have restored Active Directory, the IIS metabase, and other components. See the Exchange documentation for further details.

4. Reinstall Exchange using disaster recovery mode if you do not have a full-drive backup available for restore, and Active Directory is installed on a separate machine. The disaster recovery mode in Setup reads the Active Directory, and restores as many settings as possible. For example, database paths are stored in Active Directory, and they are set correctly whether or not you install Exchange program files to the previous locations.

   **Note:** If you restore full-drive backups and System State information, you do not need to run in disaster recovery mode. The local Exchange installation may be completely functional already. When you use disaster recovery mode, you must manually select all of the components that were previously installed on the server.

   Setup uses Disaster Recovery (DR) switches when it enters disaster recovery mode.

   For Exchange 2007/2010/2013, the DR syntax is: `/mode:recoverserver`

5. Restore the Exchange databases.

4.3 Restoring the Exchange Data

If you have backed up an Exchange database, you can choose to restore the database to its original location, an alternate location, or to an alternate Exchange database.

If you are overwriting an existing database (which must be on the same domain), it must be unmounted and marked for “overwrite” in the Exchange Management Console.

4.3.1 Exchange 2007

If you are restoring to a new location and want to mount the database, you must first create a database in a Recovery Storage Group with a Database name by using the Exchange Management Shell. For complete details, please refer to the relevant procedures recommended by Microsoft.
The Agent/Plug-in supports the restore of entire Storage Groups and/or individual databases within a Storage Group. From a workflow perspective, the restore is basically the same whether restoring from an Exchange Full or Incremental backup. In either case, the Plug-in will only need to restore from a single backup safeset.

You can only restore to the active node of an Exchange CCR cluster. The restore will fail otherwise.

You may have manually deleted a Storage Group’s transaction log files (if they were corrupt, for example). In this case, restoring a single database to a Storage Group with more than one database could result in data loss from other databases if Exchange had not committed the removed transaction logs to the database.

### 4.3.2 Exchange 2010/2013

If you are restoring to a new location and you want to mount the database, you must first create a Recovery Database through the Exchange Management Shell. For complete details, please refer to the relevant procedures recommended by Microsoft.

The Agent/Plug-in supports the restore of the entire server or individual databases on the server. From a workflow perspective, the restore is basically the same whether restoring from an Exchange Full or Incremental backup. In either case, the Plug-in will only need to restore from a single backup safeset.

You can only restore to the active copy in a Database Availability Group. A restore to the replica copy will result in not being able to mount the database or making it active. The restored files will have to be copied to the active copy node in order to successfully mount and take precedence over the other copies. Each copy will have to be updated through the Exchange Management Console. Refer to the relevant procedures recommended by Microsoft.
4.4 Restoring a Standalone Database

Your Exchange Server standalone database is restored from a single DR safeset. You need to select the Exchange Server backup job on the CentralControl application and run the Restore Wizard.

1. Before restoring your Exchange database, unmount the database you want to restore and set it to be overwritten.

2. Select your Exchange job on the CentralControl application and click the Restore button. The Restore Wizard launches.

3. Work through the wizard, as described in the "CentralControl Operations Guide".

4. On the Restore wizard – Select Restore Objects page, select the Exchange Server check box. All Exchange objects available for restore appear in the bottom pane. Select the Exchange objects you wish to restore. When you are finished with the Select Restore Objects page, click Next or click the Options button to set the available options.

5. Selecting an object enables the Options button. Click the Options button to open the Exchange Server Restore Options panel. Selecting Hard Recovery will apply the database and replay the log files. For Exchange 2007/2010/2013, it will also roll forward any logs created since the last backup that are in the original directory as long as there are no missing or corrupt log files. Hard Recovery is selected by default.

6. Complete the job and click Finish when done.

7. For Exchange, databases must be manually mounted after restore is complete and Exchange has finished restoring the databases as well as replaying the log files.

**Note:** You should always verify that your restore is successful before mounting the stores. You do this by noting that there are no errors in the restore log file and the Windows Event Viewer Log.

**Note:** If, after a bare-metal restore, you are unable to mount the database, check the following (Windows Event Viewer Log):

If the error logs had no errors, but you received an error like C1041724, and ESE Event ID 455 and Event ID 9518. The problem may be that the System State Restore restored Exchange checkpoint files that do not reflect subsequent Exchange DR backups.

To avoid the error, you should delete all the checkpoint files from the database directory (or exclude them from System State restore) before restoring the Exchange DR backup.

This is a known Microsoft problem. See Microsoft Knowledge Base Article # 896143, “The Exchange database store may not mount in Exchange Server, and event IDs 9175, 486, 455, 413, and 5 may be logged”. 
4.5 Restoring a DAG Replica Database

Your Exchange 2010/2013 Server DAG Replica database is restored from one backup. You need to select the Exchange Server backup job in the Web CentralControl application and run the Restore Wizard.

1. Before restoring, you must make the copy on the restore server active and suspend replication to all the other copies; unmount the Exchange database and set it to be overwritten.

2. Select your Exchange job in the Web CentralControl application, and click the Run Restore button. The Restore wizard launches.

3. Work through the wizard.

4. On the Restore wizard – Select Restore Objects page, select the Exchange Server checkbox. All Exchange objects available for restore appear in the bottom pane. Select the Exchange objects you wish to restore. When you are finished, click Next.

5. Selecting an object enables the Options button. Click the Options button to open the Exchange Server Restore Options page. For Exchange 2010/2013, selecting Hard Recovery will apply the database and replay the log files and it will also roll forward any logs created since the last backup that are in the original directory as long as there are no missing or corrupt log files. Hard Recovery is selected by default.

6. Complete the job and then click Finish.

7. The databases must be manually mounted after restore is complete. After Exchange has finished restoring the databases and replaying the log files, check the restore log file and the Windows Event Viewer Application Log for errors before mounting a database.

8. Mount the database.

9. Update the Suspended copies through the Exchange Management Console or Shell.

10. After replication has completed, move the active copy back to the original node.

4.6 Storage Group and Database Selection for Restore

4.6.1 Exchange 2007

From an Exchange server name, you can browse, and select one or more Storage Groups by name. Under a Storage Group, you can select one or more databases.
Note: You may have manually deleted a Storage Group's transaction log files if any are corrupt or missing. If the transaction log files have been removed, an incremental backup after the restore will not succeed. A Full backup must be performed before attempting another incremental backup.

Restoring a single database to a Storage Group with more than one database could result in data loss from other databases.

An Options button is available when the Exchange Plug-in performs a restore.

Start Hard Recovery: When selected, the Exchange Plug-in will replay the transaction logs, and prepare the restored Storage Group to be used by Exchange. By default, this option is set to true.

If you do not use this option, the Storage Group will not be available to Exchange. The Administrator can review and check the restore and Exchange files and database, and must then manually prepare the Storage Group for Exchange. Refer to the relevant procedures recommended by Microsoft.

Next, choose what to include or exclude from the restore.
4.6.2 Exchange 2010/2013

From an Exchange server name, you can browse, and select one or more databases by name on the Restore wizard page.

**Note:** You may have manually deleted a database’s transaction log files if any were corrupt or missing. If the transaction log files had to be removed, an incremental backup after the restore will not succeed. A Full backup must be performed before attempting another incremental backup.

An Options button is available when the Exchange Plug-in performs a restore.

Start Hard Recovery: When selected, the Exchange Plug-in will replay the transaction logs, and prepare the restored database to be used by Exchange. By default, this option is set to true.

If you do not use this option, the database will not be available to Exchange. The Administrator can review and check the restore and Exchange files and database, and must then manually prepare the Storage Group for Exchange. Refer to the relevant procedures recommended by Microsoft.
4.7 Storage Group and DB Selection for Restore Destination

4.7.1 Exchange 2007 Restore Destination

Select Restore Destination: Similar to selecting a Database to restore from, here you can select a database to restore to. From an Exchange server name, you can browse, and select specific Storage Groups by name. Under a Storage Group you select a specific database.

Next you may choose to restore your backup files to their original locations, an alternate location, or to an alternate database.
See the sections that follow for information about completing the restore.

**Note:** If you are overwriting an existing database (which must be on the same Domain), it must be unmounted, and marked for “overwrite”.

In the Exchange Management Console, with a database selected, right click on Database Properties to set the option “This database can be overwritten by a restore”.

### 4.7.2 Exchange 2010/2013 Restore Destination

Select Restore Destination: Similar to selecting a database to restore from, here you can select a database to restore to. From an Exchange server name, you can browse to, and select a specific database by name.

Next you may choose to Restore your backup files to their Original Location, an Alternate Location, or to an Alternate database.

**Note:** If you are overwriting an existing database (which must be on the same domain), it must be unmounted and marked for overwrite.

In the Exchange Management Console, with a database selected, edit database option, select “This database can be overwritten by a restore”.

4.8 Troubleshooting – Restore to an Alternate Location

Symptoms:

Exchange databases restored to another location (Mailbox or Public Folder) cannot be mounted. The Database and backup logs are being retrieved, but it seems like there are no restore.env files. The database is in a dirty shutdown state, and you cannot replay log files successfully to bring it back to a clean shutdown.

Description:

The restore.env file is a checkpoint file, for being able to replay transaction logs on the server. During a Soft Recovery, the checkpoint file is used to determine where to begin replaying logs. If the file does not exist, then it will start replaying, starting with the oldest log.

Hard Recovery does not require a restore.env file. The file is only created when you restore without selecting the “Hard Recovery” option.

A restore to alternate location is not considered a typical Exchange “recovery”, so you should have no Soft/Hard Recovery options during the restore process.

When the “Restore to an alternate location” option is chosen, the Plug-in places the database and log files in the new location. This means that it is the user's responsibility to correctly use these files.

Restore to alternate location should be used if:

- A normal restore is impossible. A normal restore will not be possible if the database or log files are corrupted.

The user wants to do some lower level work on these files, e.g. use a third party tool that might extract some data (e.g. mailboxes) from databases.
5 Granular Restore for Microsoft Exchange – Sharing DR Safesets

The Agent can share 2007/2010/2013 Exchange DR backup safesets for use with the Granular Restore for Microsoft Exchange application. Once a DR safeset is shared, the Granular Restore application can be used to restore individual mailboxes and messages to a .pst file.

Note: This guide provides instructions for performing tasks using legacy CentralControl applications. For instructions using Portal, see the Portal online help.

5.1 Sharing a DR Safeset for Granular Restore with Windows CentralControl

1. To share a DR safeset from within CentralControl, select the Agent and job you wish to restore from. Right-click and select Restore.

2. This will launch the Restore wizard. Here you are asked to “Choose what you want to restore”.

3. Select the Mailboxes, messages and other Exchange objects. Click Next.

Note: If the Granular Restore application is not found on the system, a warning message is displayed.

4. Select the Source and safeset from which to restore. The Source default will display the appropriate setting from the safeset backup. You can select a different safeset to restore, or a different source location. If the backup was encrypted, you must enter and confirm the password.

5. Advanced Share Options will allow you to provide sharing options for the data source. To access the advanced share options click the Advanced Share Options button.

   • Idle time: Enter the number of minutes that the share can be idle before it is automatically unshared (value can be from 2 to 180 minutes). The default idle time is five minutes.

   • Bandwidth Options: Use all available bandwidth is checked by default.

6. Click OK when your selection is complete. The Restore Job Share summary page is displayed for your review.

7. Click Share to create the share and display the share path. You should copy the share path so that you can paste it into the Granular Restore application. To copy the share path, click once to highlight the path, then right-click to copy the path to your clipboard.

8. Click Start Recovery to launch the Granular Restore for Microsoft Exchange application.
5.2 Sharing a DR Safeset for Granular Restore with Web CentralControl

1. To share a DR safeset from within Web CentralControl, select the Agent and job you wish to restore from. Click the Run Restore button.

2. This will launch the Restore from Backup Wizard. Here you are asked to “Choose what you want to restore”.

3. Select the Mailboxes, messages and other Exchange objects. Click Next.

4. Select the Source and safeset from which to restore. The Source default will display the appropriate setting from the safeset backup. You can select a different safeset to restore or a different source location. If the backup was encrypted, you must enter and confirm the password.

5. Advanced Share Options will allow you to provide sharing options for the data source. To access the advanced share options click on the Advanced Share Options button.
   - **Idle time:** Enter the number of minutes that the share can be idle before it is automatically unshared (value can be from 2 to 180 minutes). The default idle time is five minutes.
   - **Bandwidth Option:** Use all available bandwidth is checked by default

6. Click OK to save the Advanced Share Options. Click Next when your selection is complete. The Restore Job Share summary page is displayed for your review.

7. Click Share to create the share and display the share path. You should copy the share path so that you can paste it into the Granular Restore application. To copy the share path, click once to highlight the path, then right-click to copy the path to your clipboard.

8. You can now use the Granular Restore application to restore mailboxes and messages to a .pst file.
6 Appendix

6.1 Backup Considerations for Exchange 2007 CCR and LCR Setups

The Agent must be installed on both the Active and Passive nodes.

The Cluster Plug-in is not used for LCR as there is no shared storage.

For Disaster Recovery protection, you must back up:

- The entire C: drives (system state and data) on both the Active and Passive nodes.
- Exchange database

Note: There may be other dependencies/computers in your scenario that should be backed up as well: Active Directory, DNS, and Certificate Services.

Important: The Agent Service running on the Passive Node(s) must have the appropriate permissions to access the Active Exchange instance in order to obtain information regarding the mount status of databases.

WORKAROUND: The agent services (BUAgent and VVAgent) should be running as a domain user with the following permissions: (Domain Administrator account will satisfy these requirements)

Exchange View-Only Administrator

Local administrators group (for the active node)

6.1.1 Disaster protection for LCR

- LCR requires a single installation of the Agent.
- For Disaster Recovery protection, you must back up:
  - The entire C: drive (system state and data)
  - Exchange database
  - Exchange Administrator permissions are required.

Note: There may be other dependencies/computers in your scenario that should be backed up as well: Active Directory, DNS, and Certificate Services.

6.1.2 Exchange 2010/2013 Database Availability Group (DAG)

- The Agent must be installed on a DAG member containing copies of the databases to be backed up.
- The Cluster Plug-in is not used because there is no shared storage.
- For Disaster Recovery protection, you must back up:
  - The entire C: drives (System State and data) on both the Active and Passive nodes (open-file management should be used)
Note: There might be other dependencies/computers in your scenario that should be backed up as well (e.g., Active Directory, DNS, and Certificate Services).

Important: The Agent Service running on the DAG member must have sufficient permission to access the Active Exchange instance in order to obtain information regarding the mount status of databases.

WORKAROUND: Run the Agent services (BUAgent and VVAgent) as domain users with the following permissions. (Domain Administrator account will satisfy these requirements.)

- Exchange View-Only Administrator
- Local administrator group (for the Active node)

6.1.3 Restore Considerations

Disaster recovery for CCR

1. (If necessary) Re-install OS to the machine where Active Directory, DNS and Certificate Services will reside.
3. Re-install OS for each CCR node where Exchange will reside.
4. Restore the System state and data job to node 1. Re-boot on prompt. (Your original static IP’s should be restored at this point.)
5. Restore the System state and data job to node 2. Re-boot on prompt. (Your original static IPs should be restored at this point.)
6. You may need to re-start cluster services.
7. Restore the Exchange database.

Disaster recovery for LCR:

1. (If necessary) Re-install OS to the machine where Active Directory, DNS and Certificate Services will reside.
3. Re-install OS to the machine where Exchange will reside.
4. Restore the System state and data job (Re-boot on prompt)
5. Restore the Exchange database.