

Protecting Exchange 2010

Introduction

With the introduction of Exchange 2010, many new Exchange features have been added or refined in the areas of mailbox recovery, mail archiving, and system robustness. With the dataStor Enterprise Protection Server or dataStor Professional Single Server, you can protect your data while still making the most of these new features.

Before you create your backup plans to protect Exchange 2010, analyze what types of recovery you will want, then configure the system to backup appropriately. For example, with Exchange features such as Lagged Copy databases, individual mailbox backups and restores may no longer be the primary goal of the dataStor Protection plan, as a Lagged Copy can be configured to commit data for up to 14 days behind the production database. You may wish to plan for disaster recovery instead, or plan to use dataStor Exchange backups for restore requests outside of the 14 day window. You can still recover a single mailbox or even a single message with any of the dataStor Exchange backups, fully protect a single Exchange database, or the databases configured in Data Availability Groups.

Another consideration is whether to protect an active or inactive (healthy) database configured in a Data Availability Group. When using Data Availability Groups, dataStor will protect either active databases or inactive (healthy) databases that are applying replicated data from the active database. By protecting inactive (healthy) databases instead of the active databases, load balancing may be achieved, as the inactive database can be fully protected and used for data recovery up to and including complete disaster recovery.

This document will cover the planning, protection and recovery of Exchange databases, using the datastor products, for simple mailbox recovery as well as complete disaster recovery.

Disaster Recovery Planning

Protect Domain Controller

In all cases protecting your Exchange data through the dataStor product will be the same. However, for Disaster recovery scenarios you will want to protect your complete Exchange server or servers, and your domain controller for later use with a Computer System disaster recovery process.

Protect Computer System Running Exchange

A Computer System plan type integrates with appropriate VSS writers to provide a complete system backup to be used during system recovery, also known as bare metal recovery. When running a Computer System protection plan on Exchange Servers, you will need to protect the individual Exchange / Active Directory server or the Exchange server and Active Directory servers involved in the Exchange Server Organization . When you are protecting Exchange components in a File System Protection Plan,

or Computer System Protection Plan, on each Exchange servers you, should exclude your mailbox / database directories.

Finally, you will need to also refresh these backups anytime the Active Directory has been changed, through the addition of new users or mailboxes. The Exchange backups should be performed on a regularly scheduled basis, allowing for the latest Exchange backup to be used at the time of recovery.

Protect Exchange

The Exchange protection plan will protect all required Exchange files for each of the selected databases. The software queries Exchange for their location; there is no need to set up specific folders. When you run the plan, a progress update will be displayed in the User Interface.

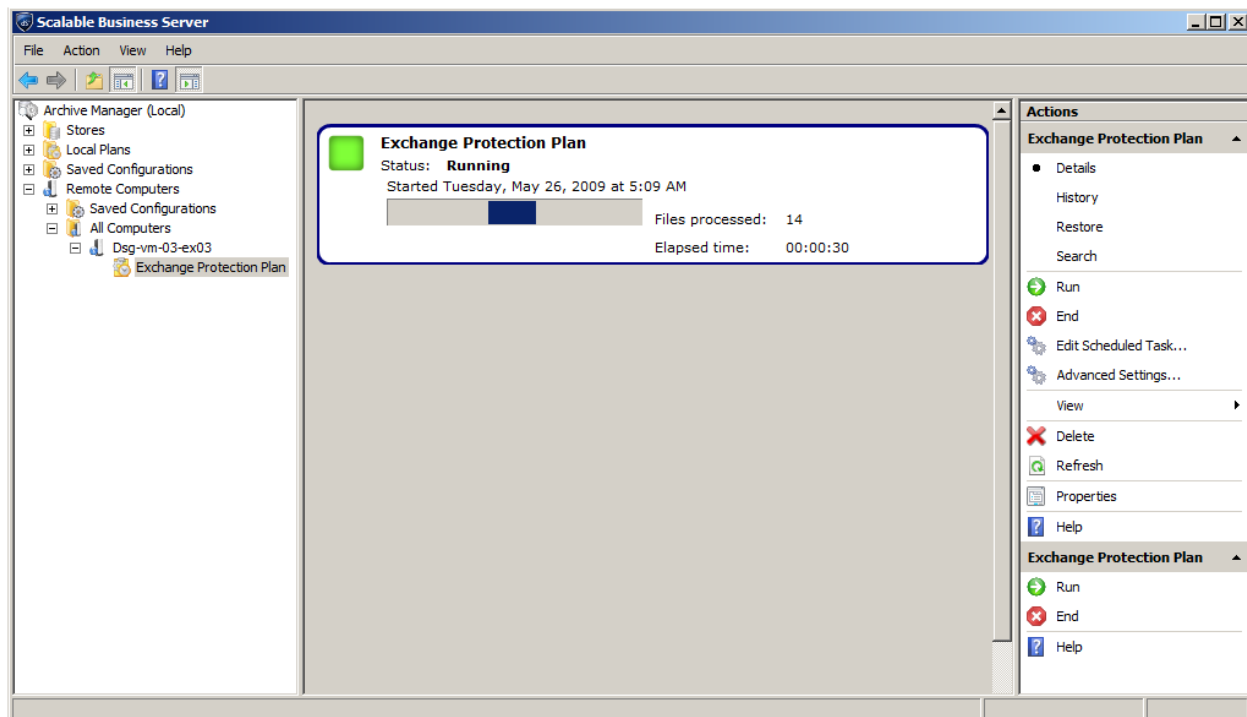


Figure 1: Progress Update.

After the plan runs, eligible logs are truncated. The History selection will allow you to see de-duplication and compression statistics.

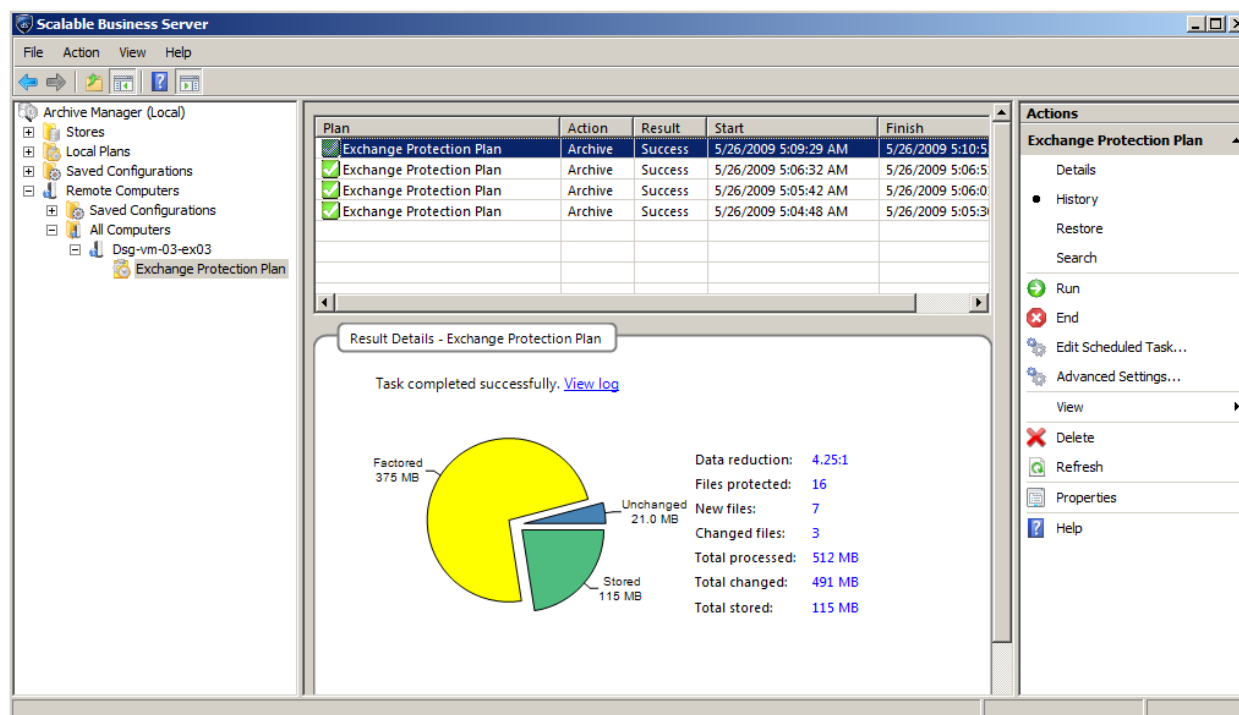


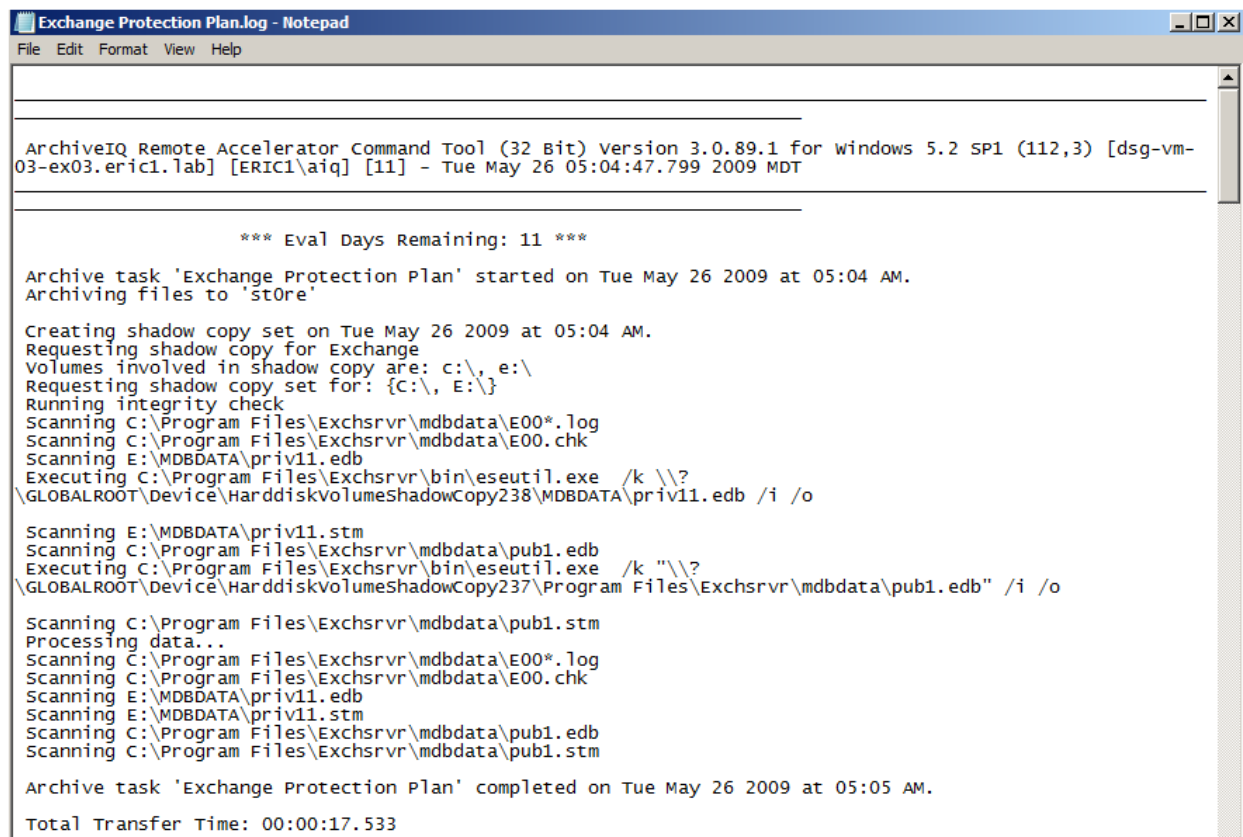
Figure 2: Storage Statistics.

Alternate Protection Strategy

The most efficient Exchange backup strategy combines an Exchange protection plan with a Files and Folders type protection plan that only captures log files for the selected database. In this scenario, the Exchange protection plan runs periodically, capturing all files necessary to restore a database as it exists at that point-in-time. The Log plan runs between Exchange plan runs, capturing log files alone. During a recovery, all logs files through the latest Log plan run may be read into the database. This strategy has several advantages, including a small backup window for Log plan runs, allowing it to run many times a day and minimizing potential data loss, and requiring the least amount of disk space over time, since large EDB files are processed less frequently.

- Add a Files and Folders type protection plan, making sure you are capturing the correct log files for the correct Exchange Storage Group. After the Exchange plan completes its first run, view the plan log and note the location of the Exchange log files for each Storage Group. To view the plan log, select the Exchange protection plan, then select the History action. In the Result Details pane, click View log.

Note the path to the log files.



```
Exchange Protection Plan.log - Notepad
File Edit Format View Help

ArchiveIQ Remote Accelerator Command Tool (32 Bit) version 3.0.89.1 for windows 5.2 SP1 (112,3) [dsg-vm-03-ex03.eric1.lab] [ERIC1\aiq] [11] - Tue May 26 05:04:47.799 2009 MDT

*** Eval Days Remaining: 11 ***

Archive task 'Exchange Protection Plan' started on Tue May 26 2009 at 05:04 AM.
Archiving files to 'store'

Creating shadow copy set on Tue May 26 2009 at 05:04 AM.
Requesting shadow copy for Exchange
volumes involved in shadow copy are: c:\, e:\
Requesting shadow copy set for: {C:\, E:\}
Running integrity check
Scanning C:\Program Files\Exchsrvr\mdbdata\E00*.log
Scanning C:\Program Files\Exchsrvr\mdbdata\E00.chk
Scanning E:\MDBDATA\priv11.edb
Executing C:\Program Files\Exchsrvr\bin\eseutil.exe /k \\\?
\GLOBALROOT\Device\HarddiskVolumeShadowCopy238\MDBDATA\priv11.edb /i /o

Scanning E:\MDBDATA\priv11.stm
Scanning C:\Program Files\Exchsrvr\mdbdata\pub1.edb
Executing C:\Program Files\Exchsrvr\bin\eseutil.exe /k \\\?
\GLOBALROOT\Device\HarddiskVolumeShadowCopy237\Program Files\Exchsrvr\mdbdata\pub1.edb" /i /o

Scanning C:\Program Files\Exchsrvr\mdbdata\pub1.stm
Processing data...
Scanning C:\Program Files\Exchsrvr\mdbdata\E00*.log
Scanning C:\Program Files\Exchsrvr\mdbdata\E00.chk
Scanning E:\MDBDATA\priv11.edb
Scanning E:\MDBDATA\priv11.stm
Scanning C:\Program Files\Exchsrvr\mdbdata\pub1.edb
Scanning C:\Program Files\Exchsrvr\mdbdata\pub1.stm

Archive task 'Exchange Protection Plan' completed on Tue May 26 2009 at 05:05 AM.
Total Transfer Time: 00:00:17.533
```

Figure 3: View Exchange Protection Plan Log.

- Add a second, Files and Folders type protection plan that specifies the folder containing the correct log files. Right click the remote computer and select 'Add Protection Plan'.

Add the path to the log files.

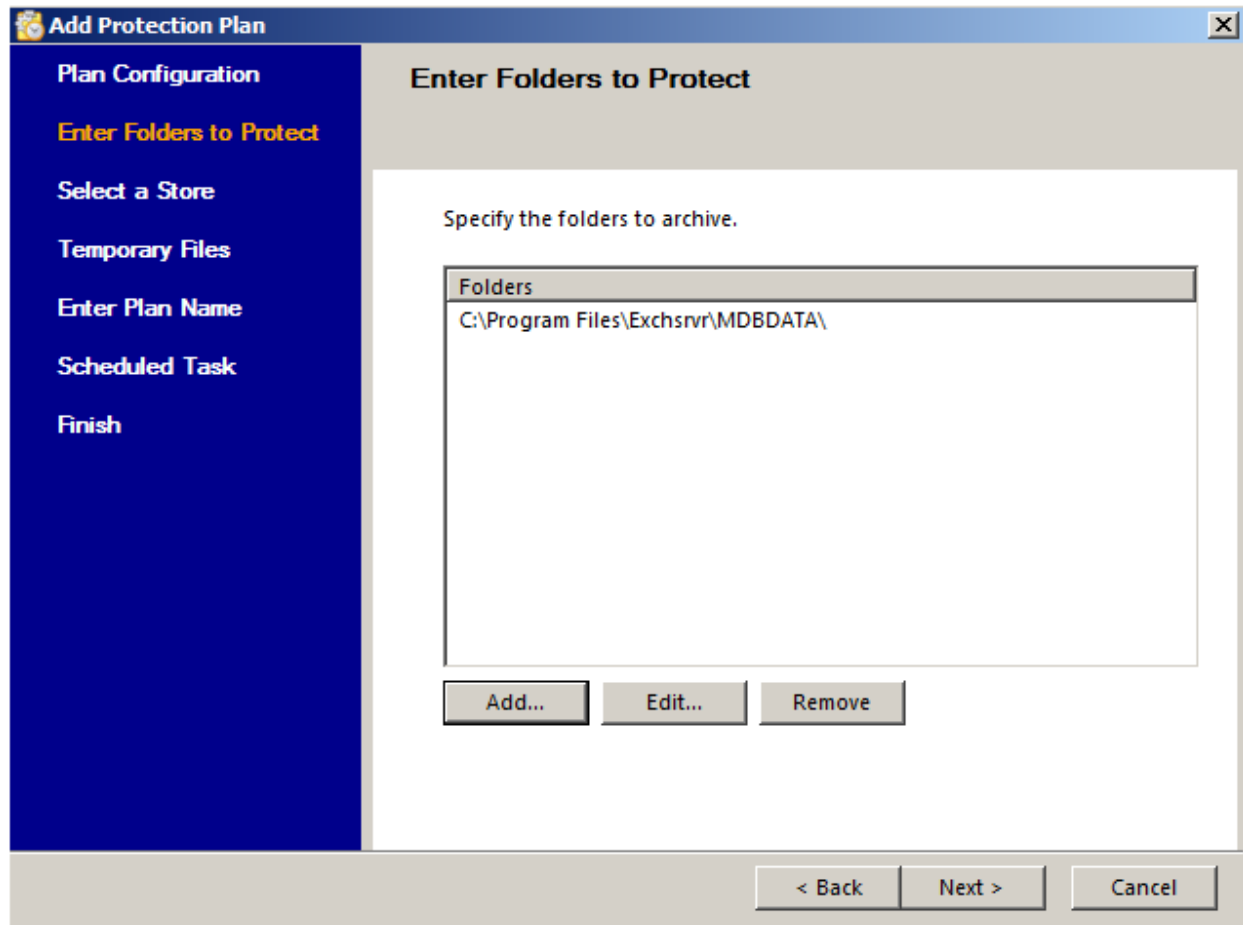


Figure 4: Add Path To Exchange Log Files.

- If the database files are located in the same directory as the log files, edit the plan to only protect log files. After the plan is created, select the plan, select the Properties action, select the Folders tab, highlight the folder selection, then click the Edit button, and append *.log to the path in the File and Folder Selection dialog box. For example, C:\Program Files\ Microsoft\Exchange Server\V14 \Mailbox\ would become C:\Program Files\ Microsoft\Exchange Server\V14 \Mailbox*.log (with no trailing backslash).

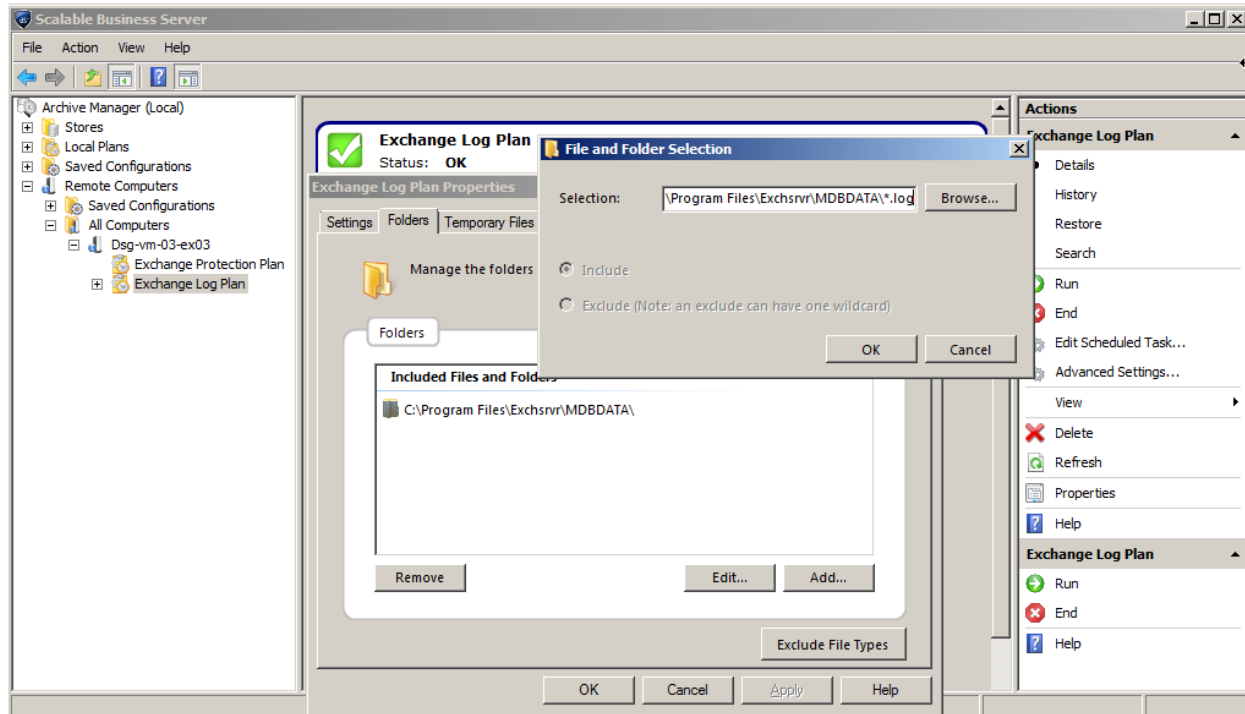


Figure 5: Edit File and Folder Selection for Exchange Log Plan

Considerations

- Schedule the log plan to run after the Exchange plan completes. Do not overlap the schedules.
- For a moderately loaded Exchange Server, consider running the Exchange plan no less than once a week. Consider running the Log plan many times a day, but all log plans for all storage groups should be timed not to run more than once every 15 minutes. For heavily loaded Exchange servers, consider setting up a Data Availability Group, and setting up a plan to protect a replica.
- To recover the most recent version of an Exchange Database, you must restore the latest restore point in the Exchange plan plus the latest restore point in the Log plan. Detailed instructions on recovery are below.
- Run through the restore procedure to become familiarized with the process.

Restore Exchange

Follow these steps to restore an Exchange Database and prepare for the recovery procedure.

1. In **Archive Manager**, select the Exchange plan, then select the Restore action. Choose a restore date in the calendar and highlight the desired restore point, and then click the Restore button.

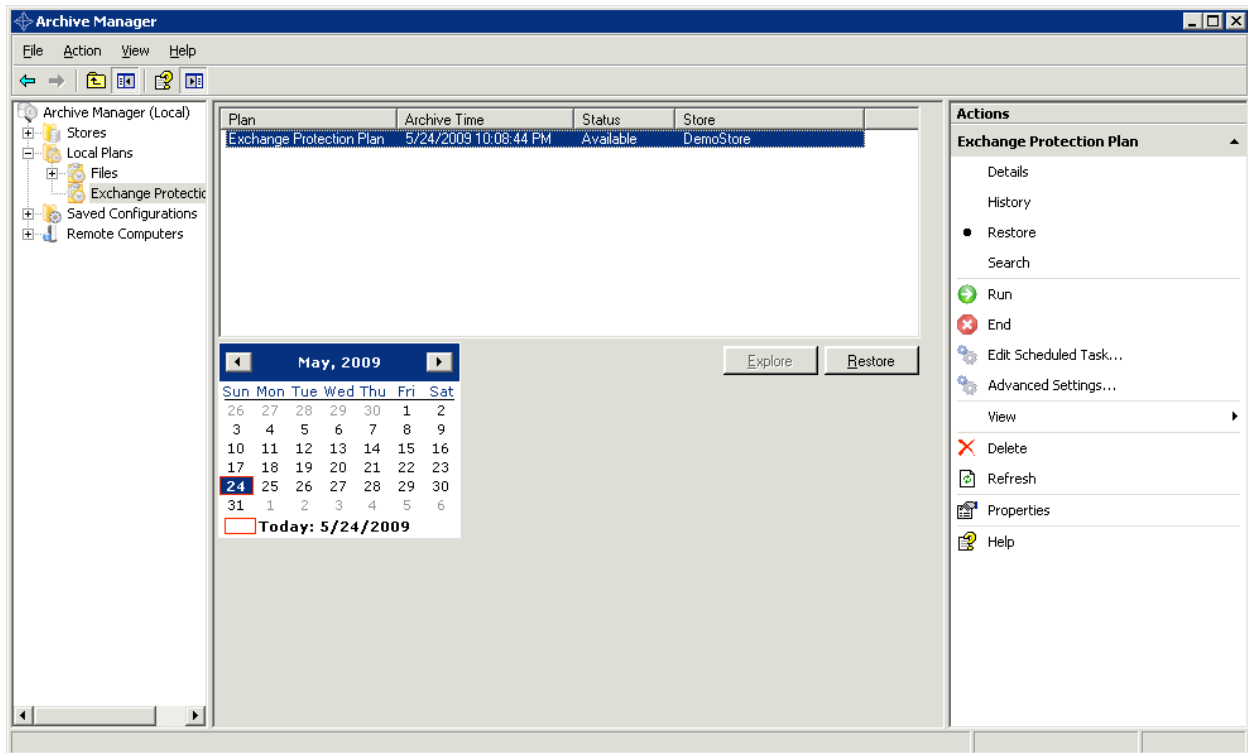


Figure 6: Select the Restore Point

2. At the Exchange Restore screen, select the Database to restore, and select a restore folder. The software restores all required Exchange files in a subfolder named with the plan name and date. The directory structure and permissions of the original Exchange Database are also restored.

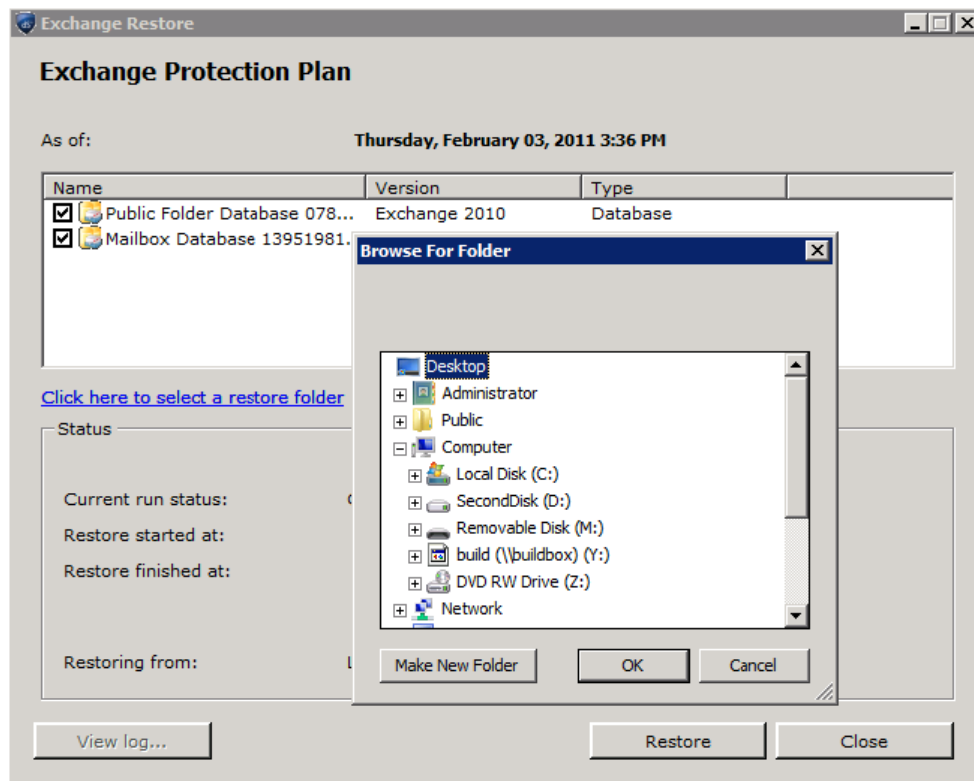


Figure 7: Select Exchange Database to Restore

Restore for Alternate Protection Strategy

If you are running a Log plan in conjunction with an Exchange plan, follow these steps to restore the files and prepare for the recovery procedure.

1. Restore the latest Exchange plan restore point following the steps outlined above.
2. In Windows Explorer, explore to the appropriate restore directory and rename or delete any file ending with .chk, tmp.log, or named Exx.log, where x will be a varying number, including 00. For example the Exx.log file for the first storage group will be E00.log. Note: to roll logs forward into the EDB file during database recovery you need a complete set of logs through the latest log file, which is always Exx.log (or the tmp.log file). Thus, the latest Exx.log file will come from the Log plan restore point, not the Exchange plan restore point.
3. Restore the latest Log plan restore point, specifying the alternate location of the date and time stamped folder under the restore folder. In **Archive Manager**, select the log plan, then select the Restore action. Choose the desired restore date in the calendar and highlight the desired restore point, then click the Restore button and follow the restore wizard. Once completed, remove any file ending with .chk. Do not remove Exx.log or the file ending with tmp.log, if present.

Recovery

When a backup application with Exchange VSS Writer integration protects an Exchange 2010 Database, Exchange marks each database file header with a Dirty Shutdown state. The header also records the log file set required to recover the database and allow it to mount successfully. Microsoft best practice is to run a soft recovery on the restored Database using ESEUtil to check the integrity of the EDB file, replay required log files into the database and mark the EDB with a clean shutdown state, ready to mount. Hard recovery is not supported. Recovered databases may be mounted as a Recovered Database, or used to replace a production database.

Disaster recovery causing the complete recovery of a database

The need for disaster recovery will come in several forms. In some cases, the servers themselves may have been destroyed, in others, you may have lost a single volume where the database resides, or you may end up with corruption on the volume, causing the server not to be able to mount the Exchange database. Microsoft Exchange 2010 has several configurations that will determine the method and style of recovery you need to perform.

Scenario # 1 – *Complete recovery of a missing Database on a single server.*

In this scenario, you may have just restored your system from a Computer System recovery plan, in which your Exchange database directories will be missing or empty. The database is unable to start.

You will need to restore your latest Exchange backup and immediately run ESEUtil /r Exx <where xx is the number of your database log prefix> /t /a /i /d . For example, **ESEUtil /r E00 /t /a /i /d**. See the **“Restore Exchange”** section elsewhere in this document for more information.

This process will apply any logs not applied while the backup was taking place, and recover your database to a state where it can once again be mounted.

When the Eseutil recovery process is complete, copy the entire contents of your database folder, to the original location on the Exchange server. This may require you to recreate the mailbox folders, depending on the exclude parameters used when creating the Computer System plan.

Once the files are copied to the original location, the database will mount and recovery is finished.

Scenario # 2 – *Corrupted databases.*

In this scenario, a volume is failing. The Exchange Server may or may not have dismounted the store, but one or many mailboxes may not be accessible, or may be missing.

In this scenario, you will want to fully understand the corruption, copy the current database, correct the issue causing the initial problem, restore your latest good backup, and mount the corrupted database as a recovery database, allowing you to copy the most current healthy data back into the system.

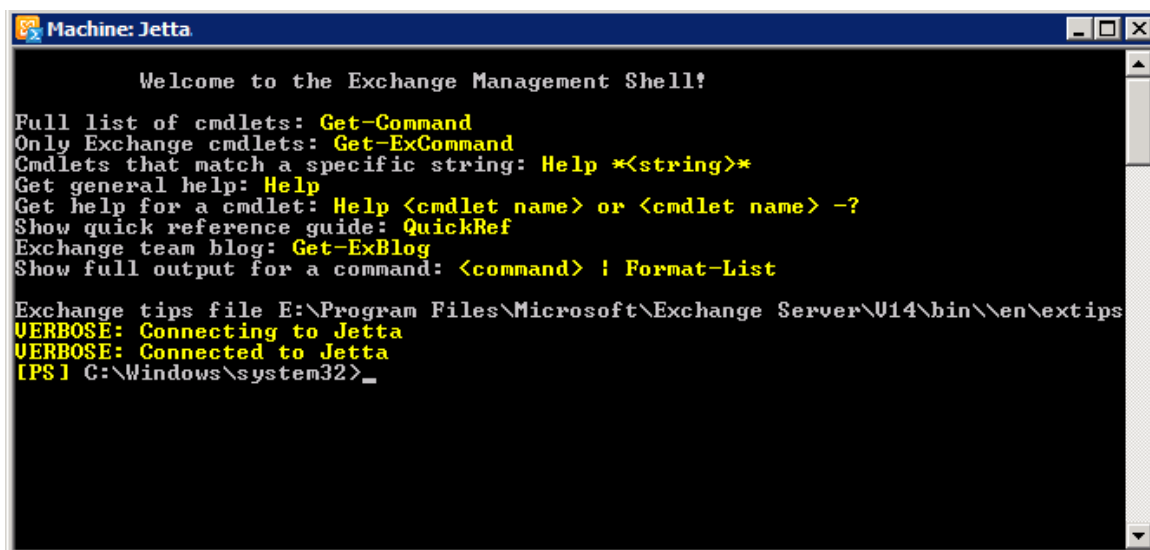
To do this, you will need to identify the corruption. If you have configured Lagged Database copies in Exchange, you may be able to roll back missing or corrupt data if the source of the corruption is not hardware related.

If rolling back data is not available, or possible, you will need to dismount the database, copy it off to a safe location, then correct the problem.

Once the problem is corrected, restore your latest good Exchange backup and recover the restored database using the command `ESEUtil /r Exx <where xx is the number of your database log prefix> /t /a /i /d`. For example, **`ESEUtil /r E00 /t /a /i /d`**. Once the recovery has been performed, copy the recovered databases back to the original location and mount the restored database. See section “**Restore Exchange**” elsewhere in this document for more information.

Next, a recovery database will need to be created in order to merge newer data from the corrupted database to the restored database. These next actions cannot be performed through the Exchange Management Console. You will need to open the Exchange Management shell for command line operations.

Open the Exchange Management Shell



```
Machine: Jetta

Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *(string)*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> ! Format-List

Exchange tips file E:\Program Files\Microsoft\Exchange Server\U14\bin\en\extips
VERBOSE: Connecting to Jetta
VERBOSE: Connected to Jetta
[PS] C:\Windows\system32>
```

Now, enter the following: `New-MailboxDatabase -Recovery -Name "<DB_NAME>" -Server <Exchange_Server> -EdbFilePath <PATH_TO_CORRUPT_DATABASE> -LogFolderPath <PATH_WHERE_LOGS_WILL_BE_CREATED>`

Example: `New-MailboxDatabase -Recovery -Name RDB1 -Server MyServer -EdbFilePath "d:\Recovery\RDB1\ILoveExchange2k10.EDB" -LogFolderPath "d:\Recovery\RDB1"`

```

Machine: Jetta

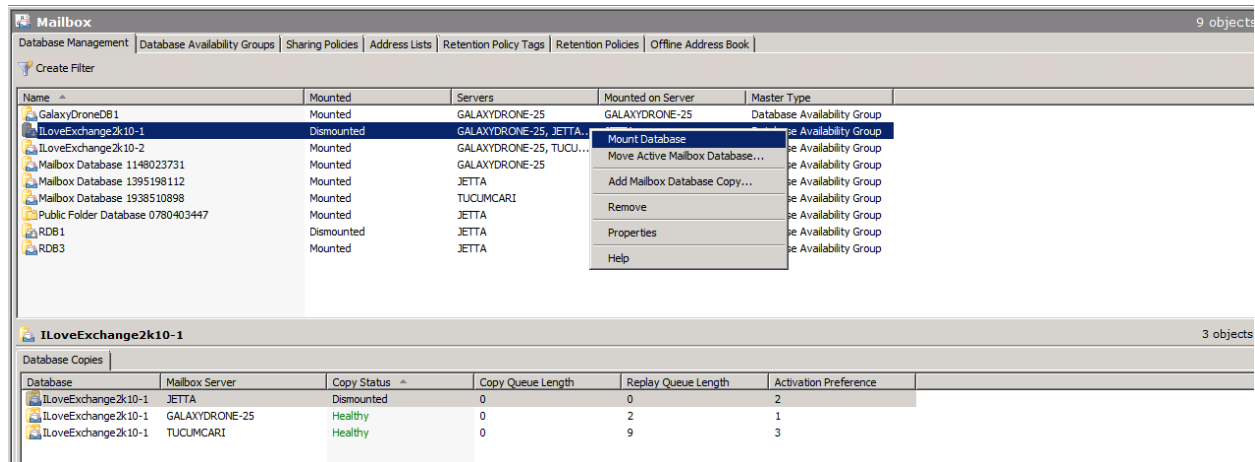
Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> ! Format-List

Exchange tips file E:\Program Files\Microsoft\Exchange Server\U14\bin\en\extips
VERBOSE: Connecting to Jetta
VERBOSE: Connected to Jetta
[PS] C:\Windows\system32>ne -MailboxDatabase -Recovery -Name RDB1
-Server MyServer -EdbFilePath "d:\Recovery\Rdb1\ILoveExchange2k10.edb"
-LogFolderPath "d:\Recovery\RDB1"

```

Once this command runs, copy the database .edb file to the EdbFilePath created in the previous command. All other files will be created when the database is mounted. In the Exchange Management Console, refresh your mailbox list to see the new recovered database and mount the database.



At this point we are able to merge data with CmdLets through the Exchange Management Shell.

- To see the list of mailboxes available in the recovery database:

Get-MailboxStatistics -Database "<NAME_OF_RECOVERY_DB> ex. "RDB1" "

- To restore a mailbox, (does not replace existing messages under Exchange 2010):

```
Restore-Mailbox -Identity <mailbox_alias> -RecoveryDatabase <recovery_database>  
-RecoveryMailbox <destination_mailbox_address> -TargetFolder  
<destination_mailbox_folder_destination>
```

Example: Restore-Mailbox -Identity JoeUser -RecoveryDatabase RDB2 -RecoveryMailbox
JoeUser@mydomain.lab -TargetFolder Inbox

If you have upgraded your server to Exchange Server 2010 Service Pack 1, the command
“Restore-Mailbox” has been deprecated.

Instead, you should use the following command:

```
New-MailboxRestoreRequest -SourceDatabase <recovery_database> -SourceStoreMailBox  
<mailbox_alias> -TargetMailbox <destination_email_address>
```

Example: New-MailboxRestoreRequest -SourceDatabase "RDB1" -SourceStoreMailBox
"JoeUser" -TargetMailbox "joeuser@mydomain.lab"

Scenario # 3 - Recovering databases in a Data Availability Group:

In Exchange 2010 Microsoft has introduced the ability to have an Exchange database replicated across several servers. In this scenario, one database will handle all transactions in and out of the Exchange server, and the other Data Availability Group (DAG) Servers will have all transactions replicated to them nearly immediately.

This scenario offers several advantages.

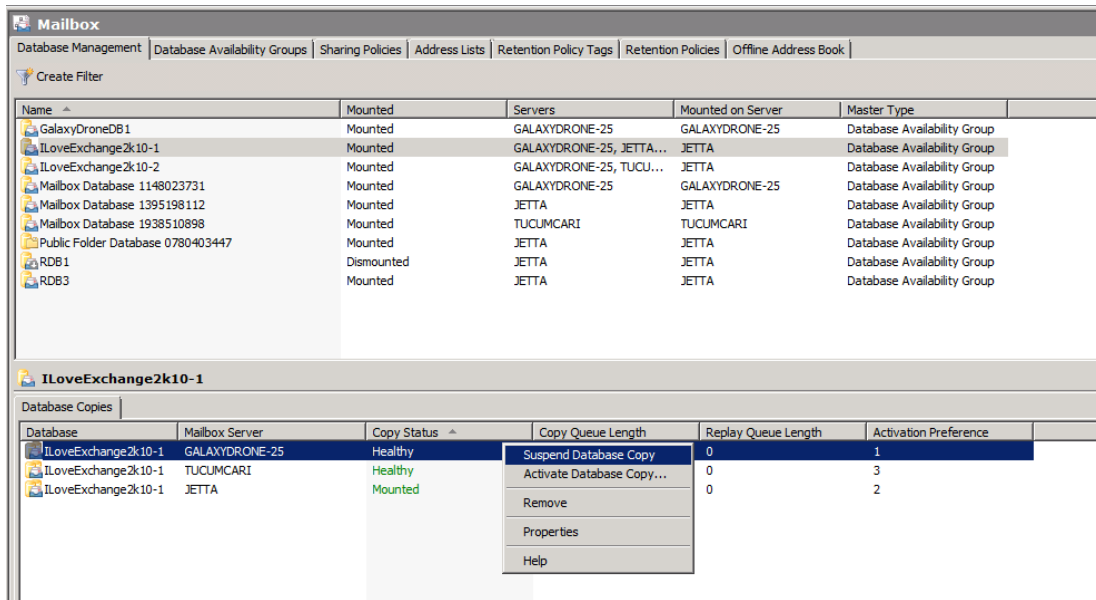
1. The ability to protect your Exchange database on a server not under load. Any available DAG server can be backed up, regardless of whether it is servicing mail requests. The dataStor products will be able to truncate the logs across all servers in a DAG once a backup is complete.
2. More generically, a Data Availability group is tied closely with the Microsoft Cluster Server. If one server becomes unavailable, the remaining servers in the DAG are able to sense the fault, and assume the primary mail handling service.

Since your databases are duplicated across several servers, only one copy of the database is needed. It is not necessary to backup and restore each server in a DAG.

If you find you need to replace the databases on a DAG, you will first need to restore the database, and recover the database. Once you have restored to an alternate directory, recover the database using the command “Eseutil.exe /r Exx /t /a /i /d” . For example, **ESEUtil /r E00 /t /a /i /d**. The logs will be

truncated leaving a stable database and any log files required to start the database. See **“Restore Exchange”** elsewhere in this document.

On each server in the DAG, dismount the active database, and Suspend database copies on each node.



Once the databases are suspended, rename or remove the folder where the mailboxes reside on each server and create a new folder of the same name. Copy all recovered files from the restore location to each folder on each server.

At this point, you will be able to mount the database on the primary server, and will need to start and synchronize the replica copies.

The best way to perform this operation is to open and use the Exchange Management Shell and execute the “Update-MailboxDatabaseCopy” cmdlet.

Run this command for each replica server. It is not necessary to run this command on each of the physical servers, but the destination server must be running, and have network connectivity.

Run the command: Update-MailboxDatabaseCopy –Identity
<Exchange_Database_Name\Node_Server_Name> -DeleteExistingFiles

For the first DAG replica server, type: Update-MailboxDatabaseCopy -Identity
"ILoveExchange2k10\myDAGServer1" -DeleteExistingFiles

For the second DAG replica server, type: Update-MailboxDatabaseCopy -Identity
"ILoveExchange2k10\myDAGServer2" -DeleteExistingFiles

At this point, your DAG servers' database copies will activate, using the restored databases. You can open the Exchange Management Console to verify the operations completed.

For more information on Exchange CmdLets used in this document, as well as other helpful commands, please visit the following links:

Update-MailboxDatabaseCopy:

<http://technet.microsoft.com/en-us/library/dd335201.aspx>

Get-MailboxStatistics:

<http://technet.microsoft.com/en-us/library/bb124612.aspx>

To list jobs in queue (may be finished)

Get-MailboxRestoreRequest:

<http://technet.microsoft.com/en-us/library/ff829907.aspx>

To clear out old jobs

Get-MailboxRestoreRequest -Status Completed | Remove-MailboxRestoreRequest

<http://technet.microsoft.com/en-us/library/ff829910.aspx>

New-MailboxDatabase :

<http://technet.microsoft.com/en-us/library/dd876954.aspx>

<http://technet.microsoft.com/en-us/library/ee332321.aspx>

Restore-Mailbox:

<http://technet.microsoft.com/en-us/library/bb125218.aspx>

New-MailboxRestoreRequest :

<http://technet.microsoft.com/en-us/library/ff829875.aspx>