HP OpenView Storage Mirroring Exchange Failover utility white paper

High availability for Microsoft Exchange Server 2000/2003

Introduction

Microsoft® Exchange Server is a messaging and collaboration server for the most demanding business needs. Its scalability, performance, and enhanced security make Exchange an ideal messaging foundation for enterprise networks. HP OpenView Storage Mirroring not only provides real-time enterprise data protection and replication but can also be used to provide high availability for your Microsoft Exchange Server.

This white paper describes the steps necessary to configure Storage Mirroring to provide high availability for Windows® servers running Microsoft Exchange Server 2000 or 2003. These procedures allow a secondary server to assume the identity and role of a failed Exchange Server while maintaining the availability of Exchange services with minimal disruption or data loss. That means that users will have access to the same mailboxes and public folders on a unique-named target server that existed on the source server before a failure.

In addition to the Exchange Information Stores (mailboxes and public folders), there are many important aspects of an Exchange Server configuration that are required for Exchange functionality following the loss of a production Exchange Server. It is important to be aware of the overall production Exchange Server configuration and to configure the target server identically. Some configuration aspects fall outside the scope of this paper, such as the configuration of any Exchange connectors, built-in Instant Messaging, Newsgroups, and Bridgehead servers. These issues need to be addressed exclusively by the Exchange administrator.

To complete these instructions, you will install Microsoft Exchange Server and Storage Mirroring then configure Storage Mirroring for replication and failover. Due to the complexities of these applications, this paper is intended for network administrators with experience installing, configuring, and maintaining network applications, including Storage Mirroring and Microsoft Exchange Server. This paper is **not** intended for Exchange running on Microsoft Cluster Service. It is for configurations with Exchange running on member servers.

Requirements

Two servers that meet one of the following operating system requirements:

- Microsoft Windows 2000 Service Pack 4 or later
- Microsoft Windows 2003

Note:
The source and target servers must both be running the same operating system.

Two licensed copies of Microsoft Exchange Server that meet one of the following requirements:

- Exchange Server 2000 with Service Pack 3 or higher
- Exchange Server 2003

Note:
It is recommended that the Exchange version be the same as the operating system version.

Two licensed copies of Double-Take 4.3.4 or later

- A copy of the Storage Mirroring Software Exchange Failover utility (exchfailover.exe) 2.0. This utility was included along with sample scripts in the application note installation package that was downloaded from the HP Support website (http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?pnameOID=439365&locale=en_US&taskId=135&prodSeriesId=439364&prodTypeId=12169).

Note:
If you are upgrading from the Exchange Failover utility 1.18, do the following:

—Compare the sample scripts to your failback and post-restore scripts and incorporate the new commands (`-nopublicfolders, -onlypublicfolders`) into your scripts.

—Modify the failover and failback scripts to remove the NSISPN commands. This functionality has been incorporated into the utility and is no longer necessary in the scripts. Leaving the commands in the scripts will not cause any harm or failure in execution.

Domain structure—The two Exchange Servers must have the same root domain.

Note:
If you are using a WAN environment (the source and target are on different subnets), see Appendix A: WAN Configuration on page 19 for additional requirements and specific WAN configuration steps.

Backing up your environment

Before beginning these procedures, be sure you have a current backup of your source and target. Also, be sure you have a complete backup of Active Directory.

Protecting your Exchange data

Protecting your Exchange data requires four separate procedures. You must complete each section before your data will be protected.

- Preparing the source server on page 4 includes the installation and preparation instructions for the source.
- Preparing the target server on page 4 installs software on the target and configures Exchange on the target.
- Configuring mirroring and replication on page 6 walks you through creating your replication set and establishing the Storage Mirroring connection between your source and target servers.
- Configuring failure monitoring on page 7 establishes high availability by configuring Storage Mirroring failure monitoring.

Preparing the source server

In this section you will configure the source and install software.

1. Configure the source as a Windows 200x member server.
2. Apply any Windows 200x service packs or patches.
3. Install Exchange 200x on the source, if it is not already installed.

Note:
Keep track of your installation selections and storage locations so that Exchange can be installed identically on the target. You must know the exact names and locations for the following items:

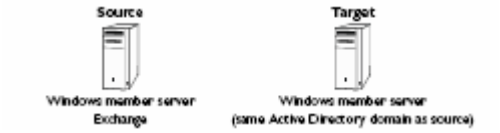
* Storage group names
* Public store name
* Private store name
* Log files and system paths
* Log file prefix
* Database names
* Database paths

4. Apply any Exchange service packs or patches. Exchange 2000 requires Service Pack 3 or later.
5. Install Storage Mirroring, if it is not already installed.
6. Run the setup.exe file downloaded from http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?pnameOID=439365&locale=en_US&taskId=135&prodSeriesId=439364&prodTypeId=12169, to install the Exchange Failover utility in the Storage Mirroring directory on the source.

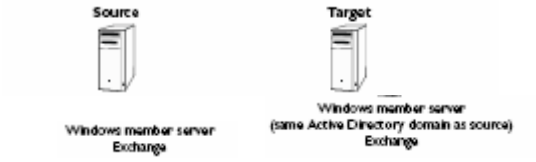
Preparing the target server

In this section, you will install software on the target and configure Exchange on the target.

1. Configure the target as a Windows 200x member server in the same Active Directory domain as the source.



2. Apply any Windows 200x service packs or patches.
3. Install Exchange 200x on the target, placing it in the same Exchange organization as the source and verifying that the installation locations are the same as the source.



4. Apply any Exchange service packs or patches. Exchange 2000 requires Service Pack 3 or later. Be sure that your Exchange installation selections and storage locations on the target are the same as the source.
5. On the target, change the Exchange services that are automatic startup to manual startup. If an Exchange service is disabled because it is not necessary for your environment, leave the service

disabled. Following is a list of Exchange services. Not all services may be used or present in your environment depending on your Exchange version.

* Microsoft Exchange System Attendant (MSExchangeSA)
* Microsoft Exchange Information Store (MSEcvhangeIS)
* Microsoft Exchange Event Service (MSExchangeES)
* Microsoft Exchange MTA Stacks (MSEcvhangeMTA)
* Microsoft Exchange Post Office Protocol (POP3Svc)
* Microsoft Exchange Internet Message Access Protocol (IMAP4Svc)
* Microsoft Exchange Management (MSExchangeMGMT)
* Microsoft Exchange Routing Engine (RESvc)
* Any other Exchange-related services: Fax, Blackberry, management software, and so on

6. When you installed Exchange on the source, the default Exchange storage group was assigned `E00` as the prefix of the log files. The second storage group was assigned `E01`, the third `E02`, and so on. The storage groups on the target must have the same numbering scheme. If you have one or two storage groups on your source, continue with the next step. If you have more than two storage groups on your source, verify that the prefix numbering is the same on the source and target.
    a. Using Exchange System Manager on the source, select the source Exchange Server. Right-click each storage group and select **Properties.** Record the prefix number assigned to each storage group.
    b. On the target, use Exchange System Manager to verify the prefix number assigned to each storage group.
    c. If the storage group prefix numbers are identical, you can continue with the next step. If the storage group prefix numbers are different, modify them. You can do this by deleting the storage groups and recreating them in the same order they were created on the source, or you can use ADSIEdit to modify the prefix numbers. Using ADSIEdit, modify the properties of the following entry noted to change the msExchESEParamBaseName on the Properties page to match that of the source. The entry that must be edited is:

```
CN=First_Storage_Group_Name, CN=Information Store,
CN=Exchange_Server_Name, CN=Servers,
CN=First_Administrative_Group_Name, CN=Administrative Groups,
CN=Exchange_Organizational_Name, CN=Microsoft Exchange,
CN=Services, CN=Configuration, DC=Domain_name, DC=com
```

    d. Install Storage Mirroring on the target and reboot when the installation is complete. This procedure will initialize Storage Mirroring and stop the Exchange service because the services are set to manual.

7. Run the `setup.exe` file downloaded from the website to install the Exchange Failover utility in the Storage Mirroring directory on the target.

Configuring mirroring and replication

In this section, you will create your replication set and establish the connection between your source and target servers.

1. On the source, open the Storage Mirroring Management Console (select **Start, Programs, Storage Mirroring, Management Console**).
2. In the left pane of the Management Console, double-click the target to log in.
3. Again in the left pane, double-click the source to log in.
4. Right-click the source and select **Properties.**
5. On the Source tab, enable **Block Checksum All Files on a Difference Mirror** and click **OK.**
6. Right-click the source and select **New, Replication Set** and enter the desired name for the replication set.
7. Select your Exchange data to replicate to the target. You can use the GUI selection process or the Replication Set Properties dialog box. For information on creating replication set rules, see the *Storage Mirroring User's Guide.*

   Note the following caveats:
   * Select the drives and/or directories that contain the Exchange database and log files. The MDBDATAS, MAILROOT, and MTDATA directories must be included.
   * Exclude the /bin directory.
   * Exclude any application files (.dll and .exe) since Exchange is already installed on the target.
   * When creating a rule that excludes files based on a wildcard, include the full path to the wildcard. For example, to exclude all .dll files in the exchsrvr directory, the replication set rule should be c:\program files\exchsrver*.dll. For information on creating replication set rules, see the *Storage Mirroring User's Guide.*

8. Right-click the replication set name and select **Save** to save the replication set.
9. Drag and drop the replication set onto the target and the Connection Manager will open.
10. The Source Server, Target Server, Replication Set, and Route fields will automatically be populated. If you have multiple IP addresses on your target, verify the Route field is set to the correct network path. (For detailed information on establishing a connection, see the *Storage Mirroring User's Guide*.)
11. Select **One to One** to map the replication set data from the source to an identical volume/directory structure on the target.
12. On the Orphans tab, select to move or delete orphan files on the source. Orphan files, such as outdated transaction logs, may keep the database from starting on the source. For more information about orphan files, see the *Storage Mirroring User's Guide.*
13. Click **Connect** to start the mirror and replication processes.

Exchange continuously writes data to the disk, which causes the replication statistics in the Storage Mirroring Management Console to constantly change, even when users are not logged in. Your data is protected after the mirror is complete and the Mirror Status has changed to **Idle**.

Note:
If you start Exchange Server and mount the replicated databases on the target, or if the data on the target is otherwise modified, the data on the source and target will no longer match. If the updated data on the target is not needed, perform a full or difference with block checksum mirror from the source to the target. If the updated data on the target is needed, restore the data from the target to the source.

Configuring failure monitoring

You will establish high availability by configuring Storage Mirroring failure monitoring. In the event of a failure, the target can stand in for the source with minimal disruption to end users.

1. If a failure occurs, have the Exchange services start on the target machine automatically. To do this, create a batch file on the target called `postover.bat` using the following sample batch file. Save the batch file to the same directory where your Storage Mirroring files are installed.

PostOver.BAT

```
rem Sample Exchange 2000/2003 post-failover script.
rem The following line pauses Double-Take processing until the Double-Take queue
rem on the target has been flushed. The time specified, in seconds, is a wait
rem time that starts when the target queue becomes idle. If the wait time
rem elapses with no further activity in the queue, processing will continue. You
rem will need to subsititute your target for target_name in the command.
"c:\program files\doubletake\dtcl.exe" waitontarget target_name 10

rem The following line sets a flag so that the database can be overwritten. You
rem will need to replace source_name with the name of your source and target_name
rem with the name of your target.
rem "c:\program files\doubletake\exchfailover.exe" -setup -failover -s source_name
-t target_name

rem The following lines start the Exchange services on the target. You may need
rem to modify the script to fit the Exchange version and specific services used
rem in your environment. If the service is running on the source, then you'll rem
rem need to start it in this batch file. If the service is not running on the rem
rem source, because it is disabled (like POP3Svc and IMAP4Svc are disabled by rem
rem default in Exchange 2003), then you do not want to start the service in the
rem batch file. If you modify the batch file to fit your environment, the rem rem
rem services must still be started in the order shown. Just remark out the rem rem
services that are not applicable to your environment. Because the Exchange rem
services may return that they have started when in fact they have not, the rem
DTCL wait command pauses processing to allow Exchange to complete its startup rem
ensuring dependent services will not fail. The amount of time to set the wait rem
command will vary from server to server. This sample script includes a 20 rem
second interval but it may need to be adjusted to fit your environment. See rem
the Storage Mirroring User's Guide for details on the wait command and rem rem
running DTCL from a command line. If desired, you can substitute the rem rem rem
Microsoft sleep utility for the DTCL wait command. The sleep utility can be rem
found in the Windows 200x resource kit.
net start MSExchangeSA
"c:\program files\doubletake\dtcl.exe" wait 20000
net start MSExchangeIS
"c:\program files\doubletake\dtcl.exe" wait 20000
net start MSExchangeMTA
"c:\program files\doubletake\dtcl.exe" wait 20000
net start POP3Svc
net start IMAP4Svc
net start MSExchangeMGMT
net start RESvc
net start MSExchangeES
net start W3SVC
net start SMTPSVC

rem The following line points the mailboxes in active directory to the target
rem server. You will need to replace source_name with the name of your source and
rem target_name with the name of your target.
"c:\program files\doubletake\exchfailover.exe" -failover -s source_name -t
target_name
```

Note:
In some cases the Information Store may not start on the first attempt. If this happens, restart the service and it should start properly. (You will have to restart the other services in the same order as listed in the script.)

The Exchange Failover utility as used in the preceding sample script is only valid for simple Exchange configurations in which the mail store names (specifically the filename of its database, excluding path information) are unique. If your environment uses the same store name for different groups or if you need to rename stores or groups on the target during failover, add additional options to the Exchange Failover utility used in the `postover.bat` script. For more information, see Appendix C: Configuring additional Exchange Failover utility options on page 24.

A copy of this sample script (`postover.bat.sample`) is available in the Samples folder, located in the directory where Storage Mirroring is installed. After you modify the sample script, copy the script and save it with a new name to remove the `.sample` extension.

If you are upgrading from the Exchange Failover utility 1.18, the failover and failback scripts can be modified to remove the NSISPN commands. This functionality has been incorporated into the utility and is no longer necessary in the scripts. Leaving the commands in the scripts will not cause any harm or failure in execution.

2. If your source server is the routing master, modify the security settings so that the routing master role can be moved to the target. If you source server is not the routing master, skip to step 3.

   You have two options available for modifying the security settings for the routing master role.

   * The first option grants the Exchange Failover utility the permission to perform the task for you. Edit the `postover.bat file` that you just created and add the –u username:password switch as outlined in the table Exchange Failover Utility Command Syntax on page 26. Specify the Exchange administrator account information.

   * The second option allows you to set the security setting manually, thus not requiring the `-u` switch in the failover and failback scripts. You will have to use ADSIEdit from the Windows Support Tools to make this change. For more information, see your Windows reference guide.

      a. Open ADSIEdit and go to CN=Routing Groups, CN=First Administrative Group, CN=Administrative Groups, CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_Name, DC=Com
      b. Right-click the entry, then choose **Properties.**
      c. Click the **Security** tab, then click **Advanced.**
      d. Click **Add.** Click **Object Types** and verify that **Computers** is selected. Click **OK.**
      e. Type in your target_name and click **CheckName.**
      f. Select **Full Control,** then click **OK.**
      g. Click the **Effective Permissions** tab, then verify the change you made (Read servicePrincipalName and Write servicePrincipalName should be selected).

3. After a failure is resolved, bring your source back online. At this time, stop the Exchange services on the target automatically and move users and roles. To do this, create a batch file on the target called `preback.bat` using the following sample batch file. Save the batch file to the same directory where your Storage Mirroring files are installed.

PreBack.BAT

```
rem Sample Exchange 2000/2003 pre-failback script.
rem The following lines stop the Exchange services on the target. You may need to
rem modify the script to fit the Exchange version and specific services used in
rem your environment, although the services must be stopped in the order shown.
net stop MSExchangeSA /y
net stop MSExchangeMGMT
net stop POP3SVC
net stop IMAP4SVC
net stop ResVC
net stop MSExchangeES
net stop W3SVC
net stop SMTPSVC
"c:\program files\doubletake\exchfailover.exe" -failback -nopublicfolders -s
source_name -t target_name
```

Note:
A copy of this sample script (`preback.bat.sample`) is available in the Samples folder located in the directory where Storage Mirroring is installed. After you modify the sample script, copy the script and save it with a new name to remove the .sample extension.

If you are upgrading from the Exchange Failover utility 1.18, do the following:
* Compare the sample scripts to your failback and post-restore scripts and incorporate the new commands (-nopublicfolders, -onlypublicfolders) into your scripts.
* Modify the failover and failback scripts to remove the NSISPN commands. This functionality has been incorporated into the utility and is no longer necessary in the scripts. Leaving the commands in the scripts will not cause any harm or failure in execution.

4. On the target, open the Failover Control Center (select **Start, Programs, Storage Mirroring, Failover Control Center**).
5. Select the target machine from the list of available machines. If the target you need is not displayed, click **Add Target,** enter the machine name, and click **OK.**
6. Click **Login** to log in to the target machine.
7. To add a monitor for the selected target, click **Add Monitor.** Type the name of the source machine and click **OK.** The Monitor Settings window will open.
8. Select the IP address to be monitored by selecting the checkbox to the left of the address in the Names to Monitor tree.
9. Select **IP Address(es)** and **Server Name** under Items to Failover.
10. Click **Account** and specify a user name and password with full domain administrative privileges, if you are failing over/back Active Directory hostname.
11. Click **OK** to go back to the Monitor Settings dialog box.
12. Click **Scripts** and specify the location and file names of the scripts previously created.
13. Click **OK** to go back to the Monitor Settings dialog box.
14. Click **OK** to begin monitoring the source machine.

In the event of a source machine failure, your target machine is now ready to stand in for the source.

Note:
If you start Exchange Server and mount the replicated databases on the target, or if the data on the target is otherwise modified, the data on the source and target will no longer match. If the updated data on the target is not needed, perform a full or difference with block checksum mirror from the source to the target. If the updated data on the target is needed, restore the data from the target to the source.

Updating Exchange components after the initial configuration

After you have completed the initial configuration and Storage Mirroring is mirroring, replicating, and monitoring for a failure, your Exchange components on the source may not be static. You may need to add a new Information Store to your Exchange configuration, or you may need to update to a new Exchange service pack. In these cases, you do not need to repeat the entire initial configuration. Use the following instructions, depending on the change you need to make.

Adding a new Information Store

1. Pause transmission from the source to the target so that you can start Exchange on the target. From the Storage Mirroring Management Console on the source, right-click the established connection and select **Transmit, Pause.**
2. Start the Exchange services relevant to your environment on the target.
3. Create the Information Store on the target with the same name and location that will be created on the source.
4. Stop all the Exchange services on the target that you started.
5. On the source, resume transmission by right-clicking the paused connection and selecting **Transmit, Resume.**
6. Create the Information Store on the target with the same name and location that will be created on the source.
7. Using the management console on the source, check the orphan settings for the established connection. Right-click the connection and select **Connection Manager.**

Note:
If you selected a path that is outside of the existing replication set, you will need to modify the replication sets on the source and target to include the paths to new data.

8. Click the **Orphans** tab and verify that you are either moving or deleting orphan files. For more information on orphan files, see the *Storage Mirroring User's Guide*. Click **OK** to close the Connection Manager.
9. Perform a file difference block checksum mirror by right-clicking the connection and selecting **Mirroring, Start.**
10. Select **File Differences** and **Use block checksum** and click **OK.**

When the difference mirror is complete, the target will be ready to stand in for the source with the new Information Store.

Applying an Exchange service pack or upgrade

1. Stop the Storage Mirroring service on the source. Any data that was already transmitted from the source but is still in queue on the target will continue to process.
2. Apply the Exchange service pack or upgrade.
3. Verify that all of the data in queue on the target has been applied to the target before continuing. You can verify that the target queue is empty by checking the Bytes in Target Disk Queue statistic in the Target section of DTState or the Bytes in Queue statistic in the Target section of Performance Monitor. If these statistics are zero, the queue is empty and you can continue. If these statistics are not zero, there is still data in queue on the target and you must wait before continuing. (For information on DTState and Performance Monitor statistics, see the *Storage Mirroring User's Guide*.)
4. Start the Exchange services relevant to your environment on the target.
5. Apply the same Exchange service pack or upgrade, ensuring that any settings applied are identical to the source.
6. Stop all of the Exchange services on the target that you started.
7. Restart the Storage Mirroring service on the source. Storage Mirroring will automatically start a difference mirror to bring the data on the target up to date with data that may have changed on the source while you were going through this process.

When the difference mirror is complete, the target will be ready to stand-in for the source with the updated components.

Dealing with a failure

If a failure occurs and the Failover Control Center Time to Fail counter reaches zero, a dialog box will appear in the Failover Control Center requiring user intervention to initiate failover. (If the Failover Control Center is not open when the failure occurs, the dialog box will appear the next time the Failover Control Center is opened. For information on monitoring a failure, see the *Storage Mirroring User's Guide*.) Acknowledge the manual intervention prompt to start failover.

The failover script created earlier will automatically run. During failover, Windows Event Viewer, Storage Mirroring log, and Exchange Failover utility logs (located in the same directory as the Exchange Failover utility) record the failover events. When failover is complete, the target will have the Exchange services started, the databases mounted, and the users pointed to the target. At this time, clients can connect through Outlook or Outlook Web Access to receive their email. Users that had Outlook open during the failure will need to restart the Outlook client (excluding Outlook Web Access clients on a LAN).

During a failover, you cannot create a new global address list because the forest-level Recipient Update Service is still pointing to the source server. Use the following instructions if you need to create a new global address list. If you do not need to create a new global address list while the target is standing in, disregard these instructions.

1. Using System Manager on the target, expand the Organization object, then expand the Recipients container.
2. Click **Recipient Update Service.**
3. In the left pane, right-click **Recipient Update Service (Enterprise Configuration)** and select **Properties.**
4. Next to the Exchange Server field, select **Browse.**
5. Locate the target server and click **OK.**
6. To manually initiate an update of the recipients in that domain, right-click the **Recipient Update Service** and click **Update Now** or **Rebuild** to force an update.

Recovering after a failure

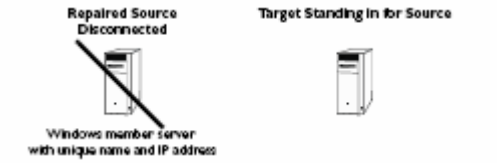
If your source experiences a failure, such as a power, network, or disk failure, your target machine will stand in for the source while you resolve the source machine issues. During the source machine downtime, data is updated on the target machine. When your source machine is ready to come back online, the data is no longer current and must be updated with the new data on the target machine.

Before you begin to restore to the original source, resolve the issues that caused the failure.

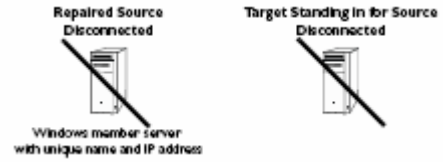
The recovery steps are different depending on the type of failure that occurred. If the source server must be rebuilt, follow the instructions in Rebuilding the source, on this page. If the server is just offline due to non-disk related issues (such as network problems or power failure) and you do not need to rebuild your server, follow the instructions in Recovering to the original source on page 15.

Rebuilding the source

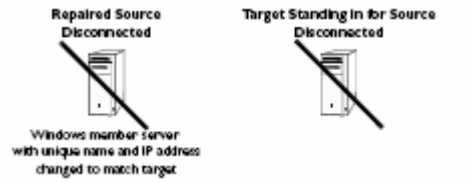
1. Install the Windows on the source, if necessary, configuring it as a Windows 200x member server with a unique name and IP address. If you need to rebuild your source using the same server name, see Appendix B: Alternate recovery method on page 22.



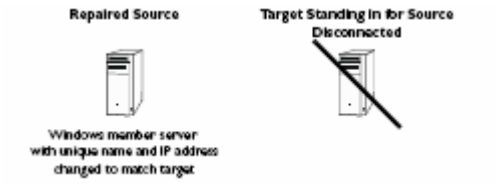
2. Apply any Windows 200x service packs or patches.
3. Temporarily, disconnect the target server from the network. At this time, users will no longer be able to access Exchange.



4. Change the source IP address to the target's assumed IP address. This is the source's original IP address before if failed.



5. Verify that the target is disconnected from the network, then connect the source to the network.

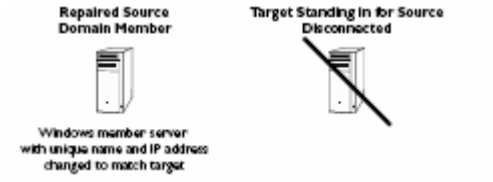


Note:
You can automate steps 6–13 and avoid rebooting by running the following two commands in a script file. Netdom is included in the Windows 200x Support Tools, found in the Support directory on the Windows 200x CD. This utility allows you to add a machine into a domain. Modify the commands to fit the names used in your environment.

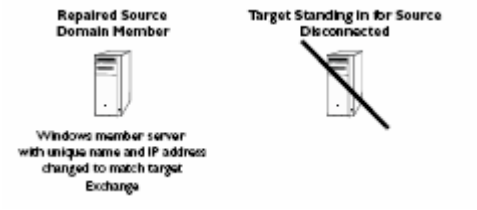
```
netdom join source_server_name /Domain:domain_name
/UserD:user_name /PasswordD:password

runas /user:user_name "cd_drive:\setup\i386\setup.exe
/DisasterRecovery"
```

If you choose to automate steps 6–13, continue with step 14.

6. On the source, right-click **My Computer** and select **Properties.**
7. Click the **Network Identification** tab and click **Properties.**
8. Under Member of, change to **Domain** and specify the domain name.
9. Click **OK.**
10. When you are prompted for a domain account, specify an account with permissions to add a workstation to the domain.
11. Reboot when prompted.



12. After the source reboots, log in as the domain administrator or an equivalent account. Verify that the account has full Exchange Administrator rights.
13. Using the Exchange CD, start the Exchange installation on the source using the following command: `<cd drive>:\setup\i386\setup.exe/DisasterRecovery`
14. At the Component Select dialog box, set the Action column to **Disaster Recovery** for all of the components that were originally installed on the source (before it failed).
15. Verify that all the components selected are installed in the same location on the source as they are on the target and the original source. If not, modify the location of each component to match the target and original source configuration.
16. After selecting the proper components and location, click **Next** to continue the install.
17. If you accepted the default installation on the original source (before if failed), set Microsoft Exchange Messaging and Collaboration Services and Microsoft Exchange System Management Tools to **Disaster Recovery**.

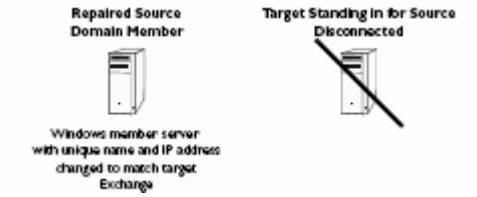


Note:
Because the Exchange disaster recovery installation is configured for tape backup recovery, informational messages such as the following may appear. However, they do not apply to this configuration and can be disregarded:

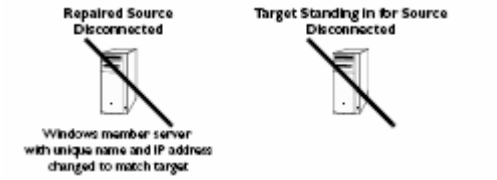
"Use Exchange Admin Snap-in to ensure that you have a valid Exchange Server Object for this server for which you are running setup in recovery mode."
"After setup has completed, restore your databases from backup, then reboot your machine."

During the post-installation processing, the installation may stall while trying to start the System Attendant (MSExchangeSA) service. It should take no more than a couple of minutes to start this service. If it takes longer, use the Windows Task Manager to terminate the setup process. This will not affect your ability to start services on the target after a failure.

18. Install any Exchange service packs or patches.
19. Install Storage Mirroring, if necessary.



20. Remove the rebuilt source from the network.



21. Reconnect the target to the network.

Recovering to the original source

1. Verify that the Storage Mirroring connection on the source has been disconnected (right-click the connection in the Management Console and select **Disconnect**).
2. Stop all of the Exchange services on the source so that you can overwrite the data with the newer data on the target. The services must be stopped in the order identified in the pre-failback script. See PreBack.BAT on page 9.
3. On the target, open the Failover Control Center (select **Start, Programs, Storage Mirroring, Failover Control Center**).
4. Select the target machine that is currently standing in for the failed source.
5. Highlight the failed source and click **Failback.** The failback script previously created will automatically run. During failback, Windows Event Viewer and the Storage Mirroring log record the failback events. When failback is complete, the Exchange services will be stopped on the target and the Failback Complete dialog box will appear.
6. Do **not** select Continue or Stop at this time. First, reconnect the source to the network.

7. After the source is available on the network, select **Continue** (to restart monitoring) or **Stop.**
8. To begin the restoration process, open the Storage Mirroring Management Console on the target (select **Start, Programs, Storage Mirroring, Management Console**).
9. Log in to the source machine by double-clicking it.
10. Right-click the original connection and select **Disconnect.**
11. Select **Tools, Restoration Manager.**
12. Complete the appropriate fields on the Restoration Manager.
    * **Original Source**—the source where the data originally resided
    * **Restore From**—the target that contains the replicated data that users have been updating
    * **Replication Set**—the name of the replication set
    * **Restore to**—the source where the data will be restored to
13. Disable **only if backup copy is more recent.** This option must be disabled because if the Exchange services were stopped on the source after the time they were stopped on the target, the source files will have a more recent date and time and the target files will not be restored.
14. Identify the correct drive mappings for the data and any other restoration options necessary. For detailed information on the restoration options, see the *Storage Mirroring User's Guide.*
15. On the Orphans tab, select to move or delete orphan files on the source. Orphan files, such as outdated transaction logs, may keep the database from starting on the source. For more information about orphan files, see the *Storage Mirroring User's Guide*.
16. Verify that the selections made are correct and click **Restore.** The restoration procedure time will vary depending on the amount of data that you have to restore.

Note:
When the restoration process is complete, the restoration status information will no longer appear in the right pane.

17. To complete the restoration process, see Running the Exchange Failover utility.

Running the Exchange Failover utility

After the restoration is complete, run the Exchange Failover utility to verify replica settings.

1. The Exchange Failover utility must be executed with the same permissions that the MSExchangeSA service uses, which is the default System permission. Open a command prompt and enter the following command:
   at \\source_name hh:mm /interactive "cmd"

   where the source_name is the name of the source and hh:mm is the current time plus one minute, formatted using a 24-hour clock. For example, if the current time is 3:00 pm., then you would enter 15:01. The command would be:
   at \\source_name 15:01 /interactive "cmd"

   In one minute, another command prompt window will open on the source console (not through Terminal Services) using the appropriate System permissions.

Note:
By default, the Terminal Services server does not allow service interaction through remote desktop.

2. In the command prompt window on the source, change to the Storage Mirroring directory and execute the following command:

   `exchfailover –setup –failback –s source_name –t target_name`
   where `source_name` is the name of the source and `target_name` is the name of the target.

3. Keep the command window open.
4. Start the Exchange services on the source.
5. If you moved the routing master role to the target, modify the security settings so that the routing master role will be updated back to the source. You have two options available for modifying the security settings for the routing master role.

   * The first option grants the Exchange Failover utility the permission to perform the task for you. If you want to use this option, add the –u username:password switch as outlined in Configuring additional Exchange Failover utility options on page 24 to the `exchfailover` command in the following step. Specify the Exchange administrator account information.

   * The second option allows you to set the security setting manually, thus not requiring the –u switch in the failover and failback scripts. You will have to use ADSIEdit from the Windows Support Tools to make this change. For more information, see your Windows reference guide.

      a. Open ADSIEdit and go to `CN=Routing Group, CN=First Administrative Group, CN=Administrative Groups, CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com`
      b. Right-click the entry, then choose **Properties.**
      c. Click the **Security** tab, then click **Advanced.**
      d. Click **Add.** Click **Object Types** and verify that **Computers** is selected. Click **OK.**
      e. Type in your `target_name` and click **CheckName.**
      f. Select **Full Control,** then click **OK.**
      g. Click the **Effective Permissions** tab, then verify the change you made. (Read servicePrincipalName and Write servicePrincipalName should be selected.)

6. In the same command window, execute the following command:
   `exchfailover –failback –onlypublicfolders –s source_name –t target_name`
   where `source_name` is the name of the source and `target_name` is the name of the target.

Note:
Depending on your configuration, this command may take several minutes to run. The interface does not provide any visual notification that the failback is in process.

You can automate steps 2–6 by using the sample batch file to automate steps after restore. If you use a batch file to automate these steps, be sure that you run it from the appropriate command prompt window (the one opened after the security group update or after the `at` command has been run). This will ensure that the batch file is run using the correct permissions.

7. Restart any Outlook clients so that they can access the source.

To reestablish protection of the Exchange data on the source, create a replication set, reestablish the Storage Mirroring connection to the target, and begin failure monitoring as previously documented in the procedure.

Sample Batch File to Automate Steps After Restore

```
rem Sample batch file to automate steps after restore.

rem The user executing this batch file must have System permissions.

rem The following line sets a flag so that the database can be overwritten. This step is
actually repetitive of previous manual steps, because testing has found the database
overwrite flag to often be inconsistent. You will need to replace source_name with the name
of your source and target_name with the name of your target.
"c:\program files\doubletake\exchfailover.exe" -setup -failback -s source_name -t
target_name

rem The following lines start the Exchange services on the source. You may need rem to
modify the script to fit the Exchange version and specific services used rem in your
environment. If the service is running on the source, then you'll rem rem need to start it
in this batch file. If the service is not running on the rem rem source, because it is
disabled (like POP3Svc and IMAP4Svc are disabled by rem rem default in Exchange 2003), then
you do not want to start the service in the rem batch file. If you modify the batch file to
fit your environment, the rem rem rem services must still be started in the order shown.
Just remark out the rem rem services that are not applicable to your environment. Because
the Exchange rem services may return that they have started when in fact they have not, the
rem DTCL wait command pauses processing to allow Exchange to complete its startup rem
ensuring dependent services will not fail. The amount of time to set the wait rem command
will vary from server to server. This sample script includes a 20 rem second interval but it
may need to be adjusted to fit your environment. See rem the Storage Mirroring User's Guide
for details on the wait command and rem rem running DTCL from a command line. If desired,
you can substitute the rem rem rem Microsoft sleep utility for the DTCL wait command. The
sleep utility can be rem found in the Windows 200x resource kit.
net start MSExchangeSA
"c:\program files\doubletake\dtcl.exe" wait 20000
net start MSExchangeIS
"c:\program files\doubletake\dtcl.exe" wait 20000
net start MSExchangeMTA
"c:\program files\doubletake\dtcl.exe" wait 20000
net start POP3Svc
net start IMAP4Svc
net start MSExchangeMGMT
net start RESvc
net start MSExchangeES
"c:\program files\doubletake\dtcl.exe" wait 20000

rem The following line points the mailboxes in active directory to the source server. You
will need to replace source_name with the name of your source and target_name with the name
of your target.
"c:\program files\doubletake\exchfailover.exe" -failback -onlypublicfolders -s source_name -
t target_name
```

Note:
A copy of this sample script (`post_restore.bat.sample`) is available in the Samples folder, located in the directory where Storage Mirroring is installed. After you modify the sample script, copy the script and save it with a new name to remove the .sample extension.

If you are upgrading from the Exchange Failover utility 1.18, do the following:

—Compare the sample scripts to your failback and post-restore scripts and incorporate the new commands (`-nopublicfolders`, `-onlypublicfolders`) into your scripts.

—Modify the failover and failback scripts to remove the NSISPN commands. This functionality has been incorporated into the utility and is no longer necessary in the scripts. Leaving the commands in the scripts will not cause any harm or failure in execution.

Appendix A: WAN configuration

Because failover of Exchange across a WAN is dependent on DNS and Active Directory, Exchange availability after failover is dependent on Active Directory and DNS updates. Therefore, additional configuration requirements and specific WAN configuration steps must be completed before the Exchange Server will be available to users. Due to the complexities of DNS and Active Directory in a WAN environment, this section of the document is intended for network administrators with experience in DNS, Active Directory, and Exchange. If you are unfamiliar with these features or are only familiar with the basics of these features, contact NSI Software Professional Services.

WAN requirements

The following additional requirements must be addressed if your source and target servers are on different subnets.

- Microsoft Exchange Server requires access to an Active Directory Domain Controller that is, at a minimum, configured as a Global Catalog Server.
- DNS Forward and Reverse lookup zones must be properly configured per Microsoft standards.

Protecting your WAN Exchange data

You must complete the same four sections as the LAN configuration to protect your Exchange data. WAN-specific steps must be completed when configuring failure monitoring.

- Preparing the WAN source server—There are no unique steps when preparing a WAN source server. Complete the same steps as outlined in Preparing the source server on page 4.
- Preparing the WAN target server—There are no unique steps when preparing a WAN target server. Complete the same steps as outlined in Preparing the target server on page 4.
- Configuring mirroring and replication—There are no unique steps when configuring mirroring or replication on the WAN source server. Complete the same steps as outlined in Configuring mirroring and replication on page 6.
- Configuring failure monitoring—Follow the steps as outlined in Configuring failure monitoring on page 7, noting three changes that must be made when configuring failure monitoring in a WAN environment:

1. On the Monitor Settings window, only select **Server Name** under Items to Failover. Do not select IP Address(es) to fail over. This corresponds to step 9 in Configuring failure monitoring on page 7.
2. Update DNS after failover. This can be done manually after failover is complete or during the failover process as part of the failover script `postover.bat` (step 1 in Configuring failure monitoring on page 7). Three possible options for updating DNS after failover are outlined in step 3.
3. Like failover, DNS must be updated after failback. This can be done manually after failback is complete or during the failback process as part of the failback script `preback.bat` (step 3 in Configuring failure monitoring on page 7).

   Three possible options for updating DNS after failback include:
   - Manual DNS updates—You can update the DNS server manually by using the Windows Administrative Tools (select **Start, Programs, Administrative Tools, DNS**).
   - Automated/Scripted updates using DNSCMD—The DNS Server Troubleshooting Tool utility (DNSCMD), which can be found in the Windows 200x support tools, can be used in the Double-Take failover and failback scripts to delete and add host and reverse lookup entries so that the source host name will resolve to the target IP address.

- For example, the following commands would be added to the end of the failover script (`postover.bat`). The second and fourth lines are identical to what appears on the PTR record's properties in the Windows 200x DNS utility.

  dnscmd dns_server_name /RecordDelete domain_name source_name A source_IP_address /f
  dnscmd dns_server_name /RecordDelete reverse_subnet_IP.in-addr.arpa reverse_lookup_IP PTR source_server_name /f
  dnscmd dns_server_name /RecordAdd domain_name source_server_name A target_IP_address
  dnscmd dns_server_name /RecordAdd reverse_subnet_IP.in-addr.arpa reverse_lookup_IP PTR source_server_name

- For example, the following commands would be added to the end of the failback script (`preback.bat`). The second and fourth lines are identical to what appears on the PTR record's properties in the Windows 200x DNS utility.

  dnscmd dns_server_name /RecordDelete domain_name source_name A target_IP_address /f
  dnscmd dns_server_name /RecordDelete reverse_subnet_IP.in-addr.arpa reverse_lookup_IP PTR source_server_name /f
  dnscmd dns_server_name /RecordAdd domain_name source_server_name A source_IP_address
  dnscmd dns_server_name /RecordAdd reverse_subnet_IP.in-addr.arpa reverse_lookup_IP PTR source_server_name

DNSCMD commands will only work if dynamic updates are enabled on the DNS zone. This is configured on the DNS zone Properties dialog box in the Windows Microsoft Management Console DNS snap-in. If **Only Secure Updates** is enabled (this option is available only on Active Directory integrated zones), the DNSCMD utility must be used in the context of a user who is in the domain DnsAdmins group. This means the Double-Take service logon account must be in the DnsAdmins group if the commands are in failover and failback scripts. The Account option in the Double-Take Monitor Settings does not apply to the failover and failback scripts, so verify the Double-Take service logon account is in the DnsAdmins group.

The Windows Dynamic DNS (DDNS) client does not initiate a registration reflecting the failed over name and IP address when failover occurs, and the `ipconfig /registerdns` command will not cause the failed over name and IP address to be registered. Accordingly, host records for the source will remain intact after failover and any required changes must be made on all DNS servers used by relevant clients. Changes to non-Windows DNS servers and Windows DNS servers with dynamic updates disabled must be implemented by some other means, but since DNS zone files are text-based, they can be manipulated with any scripting language that can open, parse, and write to a text file.

- Automated/Scripted updates using DNS WMI—The DNS WMI Provider can be used to automate or script adding and deleting records to and from the DNS server. The steps vary based on the operating system.
- Windows 2000—For information on the DNS WMI Provider, visit msdn.microsoft.com and search for DNS WMI Provider. The following link can also be used: msdn.microsoft.com/library/en-us/dns/dns/installing_the_provider.asp
- To download the DNS WMI Provider, go to: ftp://ftp.microsoft.com/reskit/win2000/dnsprov.zip
- After the DNS WMI Provider for Windows 2000 has been installed on the DNS Server, the included VBS scripts can be used to automate DNS record modifications.
- Windows 2003—The DNS WMI Provider is installed and configured by default on Windows 2003 DNS Servers, but the scripts necessary to modify DNS Records are not pre-installed. Windows Server 2003 users will still need to download DNS WMI Provider for Windows 2000, which can be found at: ftp://ftp.microsoft.com/reskit/win2000/dnsprov.zip

Dealing with a WAN failure

Just like the LAN environment, if a failure occurs and the Failover Control Center Time to Fail counter reaches zero, a dialog box will appear in the Failover Control Center requiring user intervention to initiate failover. Since your source and target servers are in a WAN environment, update your DNS records on the target so that the source points to the target's IP address. Then, acknowledge the manual intervention prompt to start failover.

Again, like the LAN environment, the failover script created will automatically run. The target will have the Exchange services started, the database mounted, and the user pointed to the target. If you did not script DNS updates in the failover script, perform the manual DNS updates at this time. When those updates are completed, clients can connect through Outlook or Outlook Web Access to receive their email. Clients who were already accessing Exchange on the source at the time of the failure may have to wait until their DNS cache is flushed and redirected to the target, or they can force the flush by using the `ipconfig /flushdns` command.

Recovering after a WAN failure

Follow the steps as outlined in Rebuilding the source on page 12, noting that there is one additional step. After step 1 and the source machine problems that caused the failure have been resolved, update the DNS records so that the source name resolves to the original source IP address. All of the remaining steps are the same for a WAN environment. When failback occurs, clients who were accessing Exchange on the target at the time of failback may have to wait until their DNS cache is flushed and redirected to the source, or they can force the flush by using the `ipconfig /flushdns` command.

Appendix B: Alternate recovery method

If you do not want to use a unique name when rebuilding the original source, use the following instructions.

1. On the target, open the Failover Control Center (select **Start, Programs, Storage Mirroring, Failover Control Center**).
2. Select the target machine that is currently standing in for the failed source.
3. Highlight the failed source and click **Failback.** The failback script created earlier will automatically run. During failback, Windows Event Viewer and the Double-Take log record the failback events. When failback is complete, the target will have the Exchange services stopped and the users repointed back to the source that you will be rebuilding.
4. Reconnect the source to the network.
5. On the target, when prompted to stop or continue monitoring of the source, select **Stop.**
6. Install Windows on the source, if necessary, configuring it as a Windows 200x member server with the same name and IP address as the original source.
7. Apply any Windows 200x service packs or patches.
8. Install Storage Mirroring, if necessary.
9. Connect the source to the network and join the domain.
    a. On the source, right-click **My Computer** and select **Properties.**
    b. Click the **Network Identification** tab and click **Properties.**
    c. Under Member of, change to **Domain** and specify the domain name.
    d. Click **OK.**
    e. When you are prompted for a domain account, specify an account with permissions to add a workstation to the domain.
    f. Reboot when prompted.
10. After the source reboots, log in as the domain administrator or an equivalent account. Verify that the account has full Exchange Administrator rights.
11. Using the Exchange CD, start the Exchange installation on the source using the following command: `<cd drive>:\setup\i386\setup.exe /DisasterRecovery`
12. At the Component Selection dialog box, set the Action column to **Disaster Recovery** for all of the components that were originally installed on the source (before it failed).
13. Verify that each of the components selected are installed in the same location on the source as they are on the target. If not, modify the location of each component to match the target and original source configuration.
14. After selecting the proper components and location, click **Next** to continue the install.
15. If you accepted the default installation on the original source (before it failed), set Microsoft Exchange Messaging and Collaboration Services and Microsoft Exchange System Management Tools to **Disaster Recovery**.

Note:
Because the Exchange disaster recovery installation is configured for tape backup recovery, informational messages such as the following do not apply to this configuration and can be disregarded.

Use Exchange Admin Snap-in to ensure that you have a valid Exchange Server Object for this server for which you are running setup in recovery mode.

After setup has completed, restore your databases from backup, then reboot your machine.

16. During the post-installation processing, the installation may stall while trying to start the System Attendant (MSExchangeSA) service. It should take no more than a couple of minutes to start this service. If it takes longer, use the Windows Task Manager to terminate the setup process. This will not affect your ability to start services on the target after a failure.
17. Install any Exchange service packs or patches.
18. Stop all of the Exchange services on the source so that you can overwrite the data with the newer data on the target. The services must be stopped in the order identified in the pre-failback script. See PreBack.BAT on page 9.
19. To complete this process, continue with step 8 under Recovering to the original source on page 15 and complete the remaining steps in that section.

Appendix C: Configuring additional Exchange Failover utility options

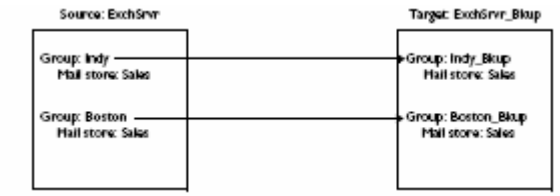
For a mail store (and its users) to be failed over (or failed back), a mail store on the source must be paired to a mail store on the target. To be a valid pair, the database filename (excluding path information) of these two stores must match. The Exchange Failover utility uses two methods to make these mail store pairs. The simplest (default) method requires that the database filenames be unique and that each filename only occurs once on the source and once on the target. This is the case for the example script provided in Configuring failure monitoring on page 7. If your environment uses the same store name in different groups or if you need to rename stores or groups on the target during failover, you will need to add additional options to the Exchange Failover utility used in the postover.bat script.

For example, a server called ExchSrvr contains two mail groups—Indy and Boston. Each group contains a mail store called Sales. In its simplest form, the Exchange Failover utility would not know which group to associate the Sales mail store with since it is based on the database filename.

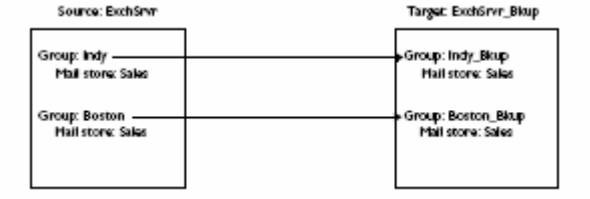
To resolve this issue, you can direct the groups and mail stores to meet your environment needs. The `-r` option in the Exchange Failover utility is a pairing rule. It allows you to specify how the groups and mail stores on the source will be paired on the target.

By itself, the `-r` option will create a one-to-one mapping from the source to the target. For example, the command `exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r` would automatically create a one-to-one mapping on the target.

You can be more specific with the `-r` option and direct the source groups to specific group names on the target. For example, the command `exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r Indy:Indy_Bkup -r Boston:Boston_Bkup` will pair the mail stores from the source Indy group in the group Indy_Bkup on the target. The mail stores from the source Boston group will be paired in the group Boston_Bkup on the target.



If needed, you can be the most specific with the `-r` option by specifying both the group and mail store names. For example, if you need to direct the group and mail store names on the target, the command `exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r Indy, Sales:Indy_Bkup, Sales -r Boston, Sales:Boston_Bkup, Sales` will pair the mail store Sales in the Indy_Bkup group from the Sales mail store from the Indy group on the source. It will also pair the mail store Sales in the Boston_Bkup group from the Sales mail store from the Boston group on the source.



There are several other options available in the Exchange Failover utility. These options and the full command syntax are included in Exchange Failover utility command syntax on page 26.

Exchange Failover utility command syntax

Command

EXCHFAILOVER

Description

Used in script files to failover Exchange data

Syntax

EXCHFAILOVER -FAILOVER | -FAILBACK -s <*source*> -t <*target*> [-l <*log_filename*>]
[-norus] [-nospn] [-nopublicfolders] [-onlypublicfolders]
[-o <*options_filename*>] [-r [<*source_group*>][,<*source_mail_store*>][:[<*target_group*>]
[,<*target_mail_store*>]]] [-SETUP] [-test] [-u <*username*>:<*password*>] [-?[?]]

Options

- FAILOVER—The Exchange data will be moved from the source to the target during failover
- FAILBACK—The Exchange data will be moved from the target to the source during failback
- s source—The name of the original source server
- t target—The name of the original target server
- l log_filename—The name of the optional log filename. By default, the log file is ExchFailover.log and is stored in the directory containing the exchfailover.exe file. If this name is changed, the DTInfo utility will not be able to locate this file, which could impede assistance through Technical Support.
- norus—Do not change the Recipient Update Service
- nospn—Do not change the Service Principle Name
- nopublicfolders—Do not move the public folders
- onlypublicfolders—Only move the public folders
- o options_filename—Allows you to pass in a file containing the options for the Exchange Failover utility
- r—By itself, this option creates a one-to-one mapping of the groups and mail stores from the source to the target
- r source_group:target_group—The `-r` option with the group names will direct the source group name specified to the target group name specified
- r source_group, source_mail_store:target_group, source_mail_store—The `-r` option with all of the `-r` options will direct the source group name and mail store specified to the target group name and mail store specified
- SETUP—Allows you to set the overwrite database on restore flag without completing user moves or RUS and folder updates. If the -setup switch is not supplied, the utility still sets the overwrite database on restore flag, but the other work is performed also.
- test—Test mode that does not change the Exchange configuration
- u username:password—A user with Active Directory permissions
- ?—Displays the syntax of the Exchange Failover utility
- ??—Displays the syntax of the Exchange Failover utility along with brief descriptions of each option

Examples

- exchfailover -failover -s Indy -t ExchSrvr_Bkup
- exchfailover -failover -s Indy -t ExchSrvr_Bkup -r

- exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales:Indy_Sales
- exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales, Inside:Indy_Sales, Inside -r Sales, Outside:Indy_Sales, Outside
- exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales:Indy_Sales -norus -u administrator:password
- exchfailover -failover -s Indy -t ExchSrvr_Bkup -o options_file.txt

Notes:

—When using the `-failback` option, the source-related options pertain to your original source or what will become the new source, if the original source had to be replaced. The target-related options pertain to the target that is currently standing in for the source.

—The password specified with the `-u` option is the only case-sensitive option in this command.

For more information

http://h18006.www1.hp.com/products/storage/software/sm/index.html

To download the Exchange Failover Utility

http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?pnameOID=439365&locale=en_US&taskId=135&prodSeriesId=439364&prodTypeId=12169

Call to action

To download a 60-day evaluation version:

http://www.openview.hp.com/products/mirror/tc_mirror_0001.html

5983-2303EN, 05/2005

invent