Technical Report

SnapManager for Exchange Business Continuance Module for Microsoft Exchange Server 2003/2007 Disaster Recovery

Niyaz Mohamed, NetApp
May 2012 | TR-4066

TABLE OF CONTENTS

LIST OF TABLES

1 Introduction

This document provides guidance on how to implement the SnapManager® for Microsoft® Exchange Business Continuance Module (BCM) for Microsoft Exchange Server 2003 and 2007 disaster recovery. This guide supplements the disaster recovery procedures listed in the SnapManager for Exchange Installation and Administration Guide.

The scope of this guide is limited to technical procedures and guidelines to support the disaster recovery of Exchange Server 2003 and Exchange Server 2007 using NetApp SnapManager for Exchange BCM.

1.1 Intended Audience

The procedures and guidance described in this document enable Microsoft Exchange administrators to utilize SnapManager for Exchange business continuance effectively. It is assumed that the audience for this document has working knowledge of the following:

- NetApp® Data ONTAP® operating system
  NetApp SnapDrive®
- Backup and restore of SnapManager for Exchange backup sets using:
  - NetApp SnapManager for Exchange (SME)
  - SnapManager for Exchange business continuance
  - Microsoft Exchange Server 2003
  - Microsoft Exchange Server 2007

2 Overview

NetApp integrates business continuance with SnapManager for Exchange (SME) to prepare for disasters, to perform failover and failback operations, and to restore Exchange databases during loss of the entire production cluster, or as a site resilience solution for a standalone Exchange Server 2003 and Exchange Server 2007, and also for Exchange 2003 virtual servers (EVSs) or Exchange 2007 clustered mailbox servers (CMSs).

SnapManager provides an exclusive business management console to define a business continuance plan, along with the ability to execute this plan, to help recover Exchange data during the disaster.

The business continuance plan can be used for routine maintenance purposes. When the production site is down, the SnapManager business management console enables the application server and moves its data to the business continuance site automatically.

This guide discusses how to implement and configure business continuance in SnapManager for Exchange for Exchange Server 2003 and Exchange Server 2007. In Exchange Server 2003, the storage-only failover and EVS failover are possible.

With Exchange Server 2007, Microsoft introduced the continuous replication features and the new data availability scenarios. Keeping this in mind, NetApp integrates the BCM functionality, so that it can be utilized in the right manner without any manual intervention. In Exchange Server 2007, storage-only failover, mailbox rehoming, and CMS failover are possible.

The purpose of this design guide is to revisit the BCM concepts and provide the necessary guidance for BCM configuration and implementation.

3 Introduction to SnapManager Business Continuance Module

The BCM feature uses the concept of source and destinations. The BCM source can be any standalone Exchange Server 2003 deployment or an active-passive cluster, an Exchange Server 2007 mailbox deployment such as a mailbox server, a single-copy cluster (SCC), or a cluster continuous replication (CCR), along with the primary storage system. The BCM destination can be a single mailbox server or an EVS or a CMS passive node, and where there is no EVS or CMS cluster configured, it should just be a passive node (standby cluster), along with the secondary storage system.

BCM uses SnapMirror® technology to mirror the storage system data and backups to a storage system in another location.

You can use SnapManager to prepare for disasters, perform failover and failback operations, and restore Exchange databases that have been destroyed or compromised. SnapManager provides an exclusive Business Management Console to define a business continuance plan and executes that plan to recover Exchange data.

3.1 General Guidance for Disaster Recovery

Consider these factors before you start with disaster recovery:

- To prepare for a catastrophic failure, keep the storage system that stores the destination SnapMirror volumes in a different physical location than your primary production system. Keep the archiving media offsite.
- Every environment and site is unique, and every company has different requirements, depending on the recovery point objective (RPO); archiving resources; and other factors such as network, Active Directory®, and so on.
- Record your Exchange data configuration and keep detailed records and logs of changes you make to your Windows® and Exchange environments.

4 Deployment Scenarios for Business Continuance

Before you create a business continuance plan, check that it is supported by your system configuration. The site failover type might be storage-only failover, mailbox rehoming (database portability), EVS or cluster mailbox server (CMS) failover, depending on your system configuration.

Supported Scenario

The following scenarios are supported:

- **Storage-only failover.** Applicable for Exchange Server 2003 and Exchange Server 2007, which utilize the underlying SnapMirror destination volumes.
- **Mailbox rehoming.** For Exchange Server 2007, the only prerequisite for moving a mailbox database between servers is that both servers must be in the same Exchange. The problems related to the user attributes affected by the database change are addressed by a parameter called “configuration only” in the move-mailbox cmdlet. For detailed requirements, see http://technet.microsoft.com/en-us/library/bb738132(v=exchg.80).aspx.
- **EVS failover.** A standby cluster is utilized to recreate the Exchange virtual instances in Exchange Server 2003. For detailed requirements on moving EVS to a standby cluster, see http://technet.microsoft.com/en-us/library/aa996470(EXCHG.65).aspx.
- **CMS failover.** A standby cluster is utilized to run /recovercms to recreate the Exchange instances in Exchange Server 2007. For detailed requirements, see http://technet.microsoft.com/en-us/library/bb738150(v=exchg.80).aspx.

Unsupported Scenario

BCM does not support the following disaster recovery (DR) scenarios:

- Mailbox rehoming is not supported on Exchange Server 2003
- Exchange Server 2007 SCC and CCR failover to CCR
- Rehoming mailboxes from standalone Exchange Server 2007 to CCR
- Rehoming mailboxes from CCR to standalone Exchange Server 2007

5 Planning and Managing SnapManager Business Continuance

Utilizing SnapManager business continuance is fairly simple and straightforward; however, there are important factors that you should consider. There are general requirements that must be met for SnapManager business continuance.

5.1 General Prerequisites for Failing Over to the Business Continuance Site

For a failover to a business continuance server, make sure that you have a valid disaster recovery plan, perform backup of all storage groups, and see that the Exchange Server is offline at the production site.

For a failover, you must first meet the following conditions:

- Create a valid disaster recovery plan.
- Perform a complete backup of all storage groups using the update SnapMirror after backup option, so that you do not lose any data.
- To simulate the BCM failover, make sure the Exchange Server is offline at the production site after you complete the backup operation.
- All servers in both Active Directory sites should be configured to use the Active Directory integrated domain name system (DNS) servers. The Active Directory replication interval for both Active Directory sites should be configured for 15 minutes.
- Make sure there are no non-Exchange LUNs in the Exchange volumes. If you configure non-Exchange LUNs in Exchange volumes, the business continuance recovery operation recovers only Exchange and SnapManager SnapInfo LUNs.
- For standalone Exchange configurations involving storage-only failover, manually dismount the storage groups in the business continuance plan prior to executing the planned failover of the business continuance plan.

5.2 Prerequisites for Creating a Business Continuance Plan

Before you create a business continuance plan for your clustered configuration or on a standalone server, make sure that you have necessary software installed, drive letters or mount points available, and the correct cluster configuration on the production and business continuance sites:

- Exchange, SnapDrive, and SnapManager are installed.
- The SnapManager service account has full access privileges.
- Make sure that business continuance is supported by your system configuration.
- The drive letters or mount points used by Exchange databases, transaction logs, Simple Mail Transfer Protocol (SMTP), Message Transfer Agent (MTA), and Exchange data directory should be available to use in the business continuance host.
- In the case of Exchange Server 2003, the Exchange data directory specified during creation of the Exchange virtual server should be in a LUN along with either SMTP or MTA components, logs, or SnapManager SnapInfo components.

- You should have created and initialized all SnapMirror relationships between the source and destination volumes.
- Before creating a business continuance plan, make sure that the mailbox database cluster resources are dependent on the appropriate disk resources, as recommended by Microsoft. This step is necessary because the installation of Exchange 2007 does not create a dependency between database resources and disk resources. This can result in some databases not appearing online after a business continuance failover. Also, after a business continuance failover, recreate the dependencies appropriately between database resources and disk resources.
- If you have a primary DNS on the production site and a secondary DNS running on the business continuance site, convert the secondary DNS running on the business continuance site into a primary DNS. This converts the secondary DNS from a read-only server to a write-enabled server, hence preventing the failure of DNS changes during the execution of your business continuance plan.
- In a remote recovery scenario, a standby Windows cluster should be used at the business continuance site.
- Make sure that the operating systems installed on both the servers are the same version and service pack.
- In Microsoft Window 2008 failover clusters, the network name resource has a new private property, HostRecordTTL, which is set to 20 minutes by default. Set the private property HostRecordTTL to five minutes as recommended by Microsoft.
- Prior to creating the business continuance plan, make sure that the Microsoft Exchange EVS version matches the version and service pack of the Exchange binaries in all of the production and DR cluster nodes. Check the store.exe version in the BIN directory on the servers.
- Prior to creating the business continuance plan, make sure that the Microsoft Exchange CMS version and service pack match the version of the Exchange binaries in all the production and DR cluster nodes. This should be done when you upgrade your version of Microsoft Exchange. Check the store.exe version in the BIN directory on the servers.
- If you are using Windows 2008, the Windows Management Instrumentation traffic should be enabled in the firewall.
- If you are using Windows 2008, the Windows Management Instrumentation namespace security must allow SnapDrive and SnapManager to access all nodes in the cluster.
- If you are using Windows 2008, the network name specified when you create the business continuance plan must match the cluster network name.
- For Windows 2003, the network name must match the network connection name.
- If you are using Microsoft Windows 2008, rename the network name in the Failover Cluster Management to be the same as the network name in the Control Panel prior to creating the business continuance policy. The Windows 2008 system uses different network names in the Control Panel and Failover Cluster Management module. During the business continuance policy creation, the network name in the Failover Cluster Management is used. This will cause the business continuance policy execution to fail when executed.

5.3 Impact of Active Directory Replication Lag on Business Continuance

If the Active Directory replication lag is more than the threshold value, the recreation of the Exchange instance can fail at the business continuance site. To avoid such errors, make sure of the following:

- The intrasite and intersite replication lags are minimum and within the threshold.
- All Active Directory replication links work properly with minimal lag. The Active Directory sites and services or repadmin and replmon command-line tools can be used to force replication.

5.4 Standby Cluster Overview

A *standby cluster* is a Microsoft Windows Server® cluster that:

- Matches the production Exchange cluster in terms of hardware and software configuration, including Microsoft Windows and Exchange versions and hotfix updates.
- Has Exchange program files installed on it, but they are not yet configured with any EVS or CMS servers.
- Can be used only when all Exchange virtual servers on the production cluster are offline.

The standby cluster will reuse the information already stored in the configuration partition of Active Directory; hence, the following requirements of an Exchange standby cluster must be met:

- The standby cluster cannot host any Exchange virtual servers or clustered mailbox servers from any other cluster.
- The operating system version is Windows Server 2003 Enterprise Edition or Windows Server 2008, accordingly.
- The operating system service pack and hotfixes installed on the standby cluster should be the same versions as those installed on the production cluster.
- It is possible to have the standby cluster installed in a different IP subnet. However, there are certain implications of this that might affect the BCM activation procedure.
- Exchange Server 2003 binaries or Exchange Server 2007 binaries, service pack, and hotfixes should be preinstalled on all nodes of the standby cluster and match the versions installed on the production cluster.
- The standby cluster node IP address(es) and computer name(s) must not conflict with any other IP addresses or computer names on the network.
- The standby cluster IP address and cluster network name resources must not conflict with the cluster IP address or cluster network name of any other cluster on the network.

For detailed requirements of standby clusters, see http://technet.microsoft.com/en-us/library/aa996470(EXCHG.65).aspx.

6 Main Site Failure and BCM Activation Workflow

If the primary site fails due to a natural calamity or for other unknown reasons, recovering the primary site takes a long time. Hence, the BCM plan needs to be executed. As the production site is down, the SnapManager Business Management Console enables you to move the affected Exchange Server and its data automatically to the business continuance site.

The following tasks are performed as part of the business continuance plan:

- Business continuance server validation
- Cleanup of business continuance destination
- Take Exchange instances offline
- Quiesce and break SnapMirror relationships
- Reconnect Exchange LUNs
- Exchange instance recreation
- Restore backups

The first step is to initialize the business continuance information and DR operations manager. As part of the initialization, information is retrieved from the business continuance plan. Once it is initialized, the business continuance information is queried to check if it is a storage-only failover, EVS failover, or CMS failover.

Best Practices

- It is best to use the same SME user account and password for this task, as it will have the correct permissions to execute the task.
- Make sure that there are no firewall restrictions between the remote and local servers.

When planning recovery time objective and recovery point objective (RTO and RPO), it is important to know the different factors that affect recovery time. Activation of BCM begins with verification of directory services and the DNS resolution. After directory services and DNS have been verified, the next step is to execute the plan, which will perform a recovery of the clustered mailbox server.

The time taken to perform a recovery varies from one environment to another, as there are many parameters that we need to consider. Some of these parameters include network, AD replication state, and so on. Ideally, site activation should take about one hour, provided the steps are followed correctly.

Workflow

Business Continuance Server Validation

Validation makes sure that the correct resources and server configurations are involved in the recovery operation.

1. The process validates business continuance host prerequisites.
2. Validates LUN connections, SnapManager SnapInfo, transaction log, and Exchange data LUN connections.
3. Checks the SnapMirror relationship information.
4. Validates the business continuance plan against existing Exchange configuration.

Cleanup of Business Continuance Destination

1. Cleans up the Exchange cluster resources and determines the LUNs to be cleaned up in the destination and then disconnects the LUNs.

Quiesce and Break SnapMirror Relationships

1. In this step, the SnapMirror relationships that need to be broken are retrieved from the business continuance plan and then broken.

Reconnect Exchange LUNs

In this step, BC initializes the business continuance cluster resource group and resources.

a. SnapManager Exchange BC checks the resource group specified in the DR plan and verifies if the network name resource with the specified name exists.

b. It also validates whether the business continuance resource group exists.

c. Clears volume mount point directories and registry settings for volumes that are no longer in the system and completes the initialization of Snapshot™ information.

d. Evaluates Exchange storage layout for volume SnapRestore® and checks if any of the Exchange volumes are qualified for volume SnapRestore.

e. Connect LUNs to the DR server and retrieve the Snapshot copies for the volume. A volume SnapRestore is performed after evaluating the Exchange storage layout. The volume SnapRestore method can be used to decrease the time required to complete the restore, while minimizing overheads on the storage controller. If not used, the LUN clone restore will be used for restoring the LUN.

After this step, all the LUNs are connected to the standby cluster.

Recreate Exchange Instances.

a. Recreate the Exchange cluster resources and retrieve the recreation strategy from strategy manager.
b. Retrieve the information about all the cluster resources in the resource group.
c. The dependency for the IP address and network name resource is removed, and the resources are deleted, respectively.
d. After the deleting the resources, create the network name and IP address resource for DR and add necessary dependencies.
e. Reset the machine account and bring the resource group online.
f. Later, BCM recreates the Exchange cluster resources and brings resource group online.

This step also configures the Exchange mailbox settings and the local DNS cache of the business continuance host.

Restore Backups.

1. This step initializes the SME server agent and retrieves the volume Snapshot information. The prerequisites for restore are verified, and the job is started.
2. Once these steps are completed, the business continuance plan execution is completed successfully, and the DR site is ready for usage with minimal downtime.

7 Creating a Business Continuance Plan

When you create a business continuance plan for recovering Exchange data, you can create it as a local or remote recovery. The plan specifies resources and other information that will be needed for recovery after a disaster occurs.

7.1 About This Task

Associate initiators for connecting each of the LUNs in the destination host. For a cluster, associate initiators for each of the LUNs to each node of the destination cluster. In a local recovery scenario, you can recover your Exchange data in the same host using a different set of storage resources. In a remote recovery scenario, you can recover the Exchange data in the remote host using a different set of storage resources.

For an Exchange Server 2007 standalone remote recovery, mailbox rehoming is done automatically. In cluster configurations with Exchange, the business continuance plan creation will also configure the access control list of the Exchange machine account, by adding access control entries for the DR cluster machine account and the cluster node machine accounts.

Best Practices

Make sure that the following requirements are met.

- All the Exchange volumes should be mirrored using SnapMirror technology.
- LUNs with exchange components such as SMTP, MTA, SEARCH instance data, and data directory (Exchange 2003) should share the storage system volume with transaction log or database or SnapManager SnapInfo LUNs so that they will be automatically backed up and replicated for business continuance.
- If you want to take advantage of volume SnapRestore for maximum recovery time objective, make sure that the following storage layout requirements are met:
  - Database LUNs should not share the storage system volume with logs, SnapInfo, SMTP, MTA, or search instance LUNs.
  - All the storage groups and databases in a backgroup will have to be backed up together.

7.2 Steps

Follow these steps to create a business continuance plan:

1. Launch the business continuance using the path Start > All Programs > NetApp > SnapManager for Exchange Business Continuance.
2. In the Actions pane, click Manage Business Continuance.
3. Select a business continuance server.

Table 1) Creating local and remote recovery plans.

If You Want to Create...	Then...
A local recovery plan	Connect to the production host and create the business continuance plan.
A remote recovery plan	Connect to the business continuance host and create the business continuance plan.

4. To select the required business continuance host, click Yes; otherwise, click No.
5. In the Actions pane, click New Business Continuance Plan.
6. In the Choose an Exchange Server page, specify the name of the Exchange Server to be enabled for business continuance.
7. In the Recovery Cluster - Resource Information page, either select an existing network name or specify the new resource details.
8. Select the Choose Existing Resources, Specify Network Name, Resource Group, IP Address, SubNet Mask, and Network type options.
9. In the Business Continuance Storage Resources page, specify the current production storage resources and the storage resources for disaster recovery.
10. For example, if the production storage resources are in data center 1 and the business continuance storage resources are in data center 2, you must first select data center 1 and then data center 2.
11. In the Business Continuance Mirrors page, select the list of SnapMirror destinations for business continuance.
12. In the Choose Initiators page, specify the initiators to use for LUN connections from the host to storage resources.
13. In the Business Continuance Plan Details page, specify the name of the business continuance plan, describe the business continuance plan, and provide the emergency contact information.
14. Click Finish.

7.3 Creation of a Business Continuance Plan for a Microsoft Exchange Server in a Site Resilience Scenario

SMEtest Ltd. has two data centers:

- A primary data center referred to as Active Directory main site that contains the following infrastructure components:
  - Directory server, SMEDC, which provides secure, Active Directory integrated DNS services
  - Exchange virtual server, EXCH, running in a two-node active or passive cluster, EXCHCLUSTER, which contains SMEE2K3N1 and SMEE2K3N2
- A second backup data center referred to as Active Directory DR site that has the following infrastructure components:
  - A Windows 2003 additional domain controller, SMEDC2, which also provides secure, Active Directory integrated DNS services
  - Standby cluster, E2K3DRCLUS, which will be used as a standby failover cluster

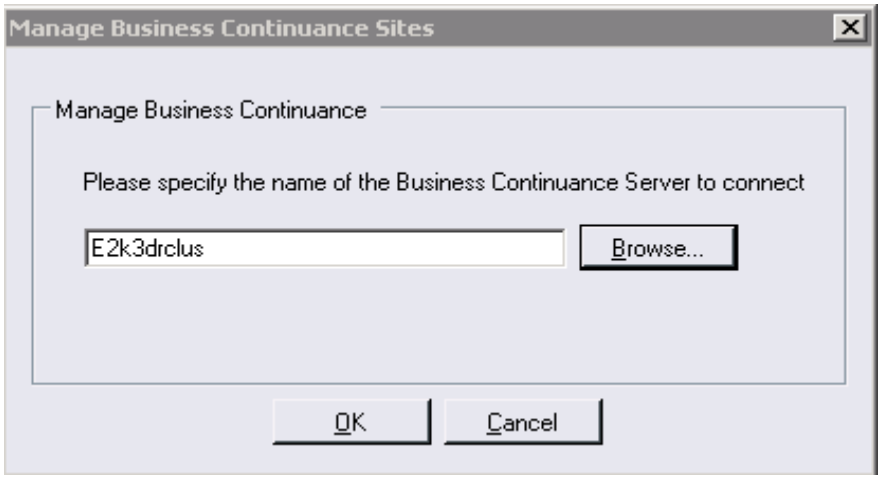
  Note: The node in this cluster, SMEE2K3DRStandby, is the only node in the standby failover cluster.

In this scenario, the primary data center fails, and SMEtest Ltd. makes the decision to activate the secondary data center using the BCM.

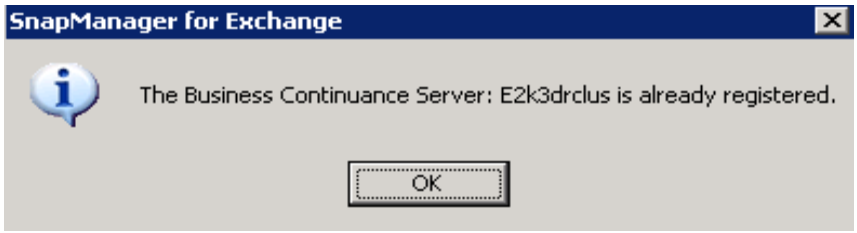
7.4 Implementation and Configuration of SME BC

Follow these steps to implement and configure SME BC:

1. Launch the business continuance page using the path Start > All Programs > NetApp > SnapManager for Exchange Business Continuance.
2. In the Actions pane, click Manage Business Continuance.
3. Select a business continuance server.

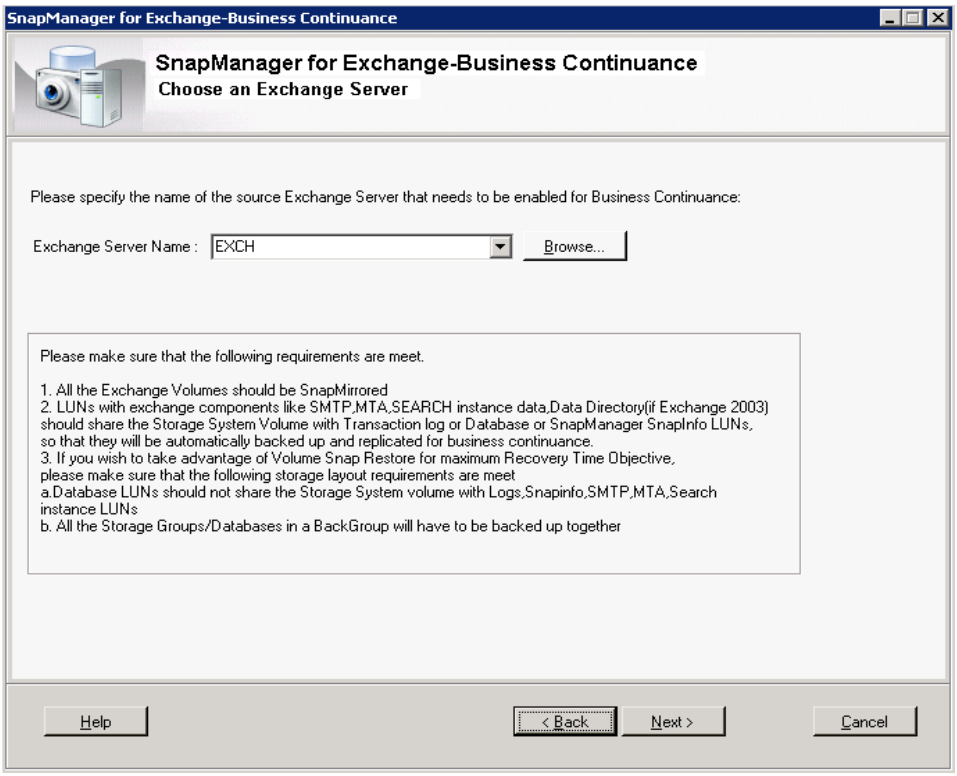


4. To proceed with the chosen business continuance host, click OK.

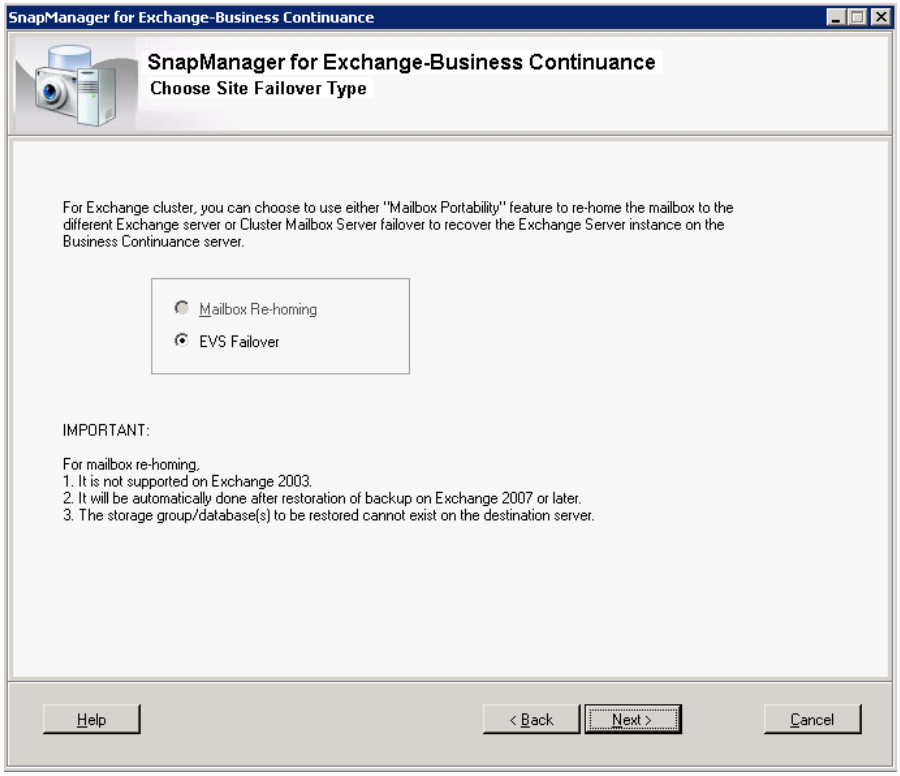


5. In the Actions pane, click New Business Continuance Plan.

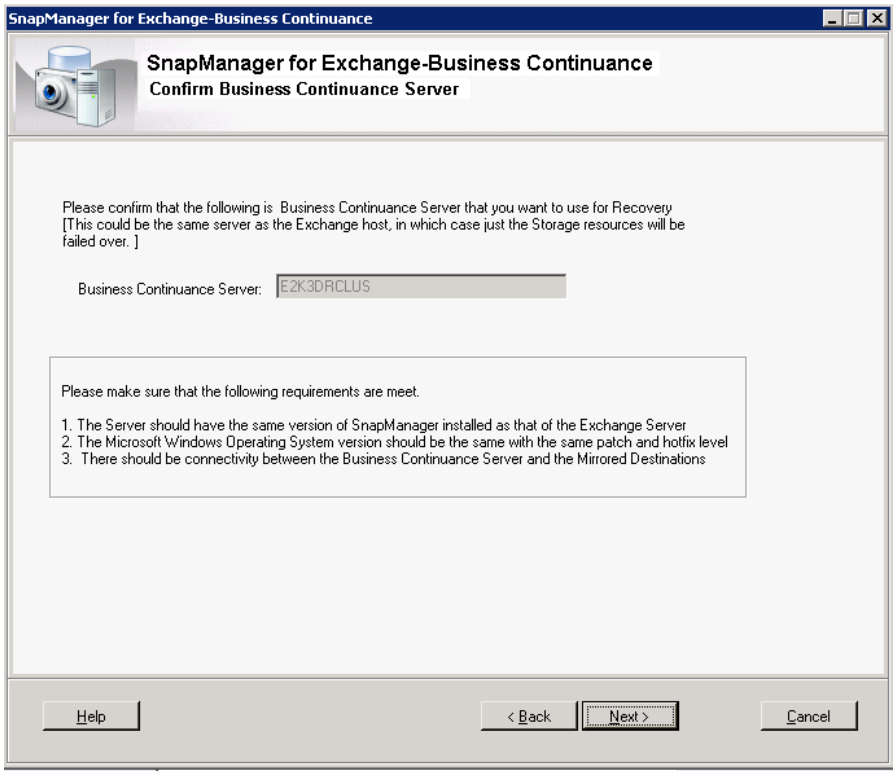
6. In the Choose an Exchange Server page, specify the name of the Exchange Server to be enabled for business continuance.



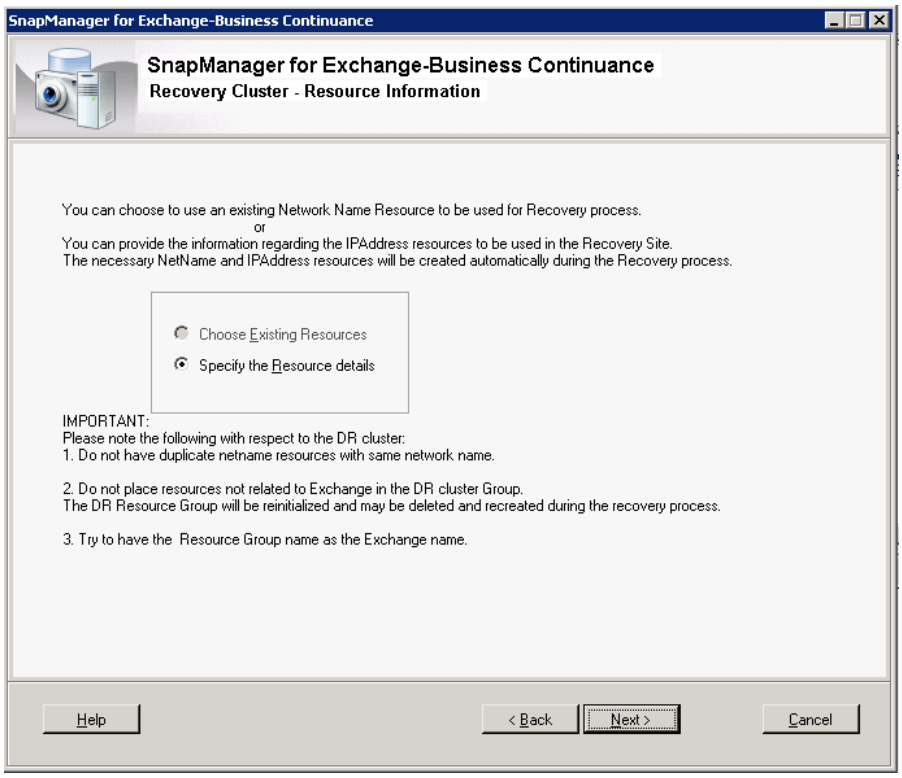
The business continuance is intelligent enough to determine the underlying cluster and provide necessary options as follows:

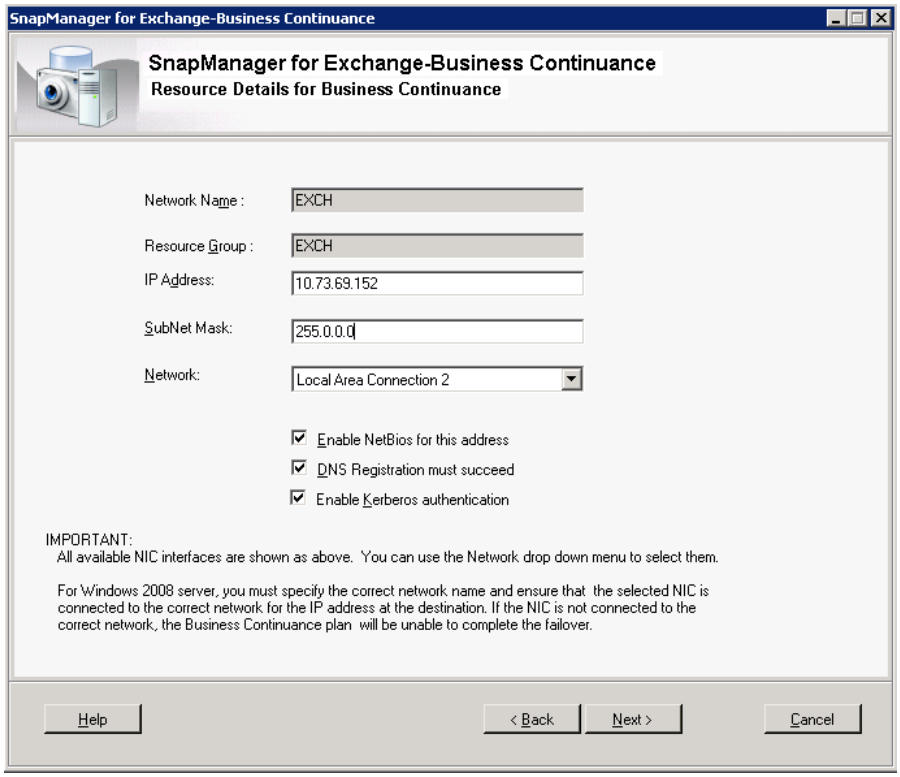


7. In the Recovery Cluster-Resource Information page, either select an existing network name or specify the new resource details.

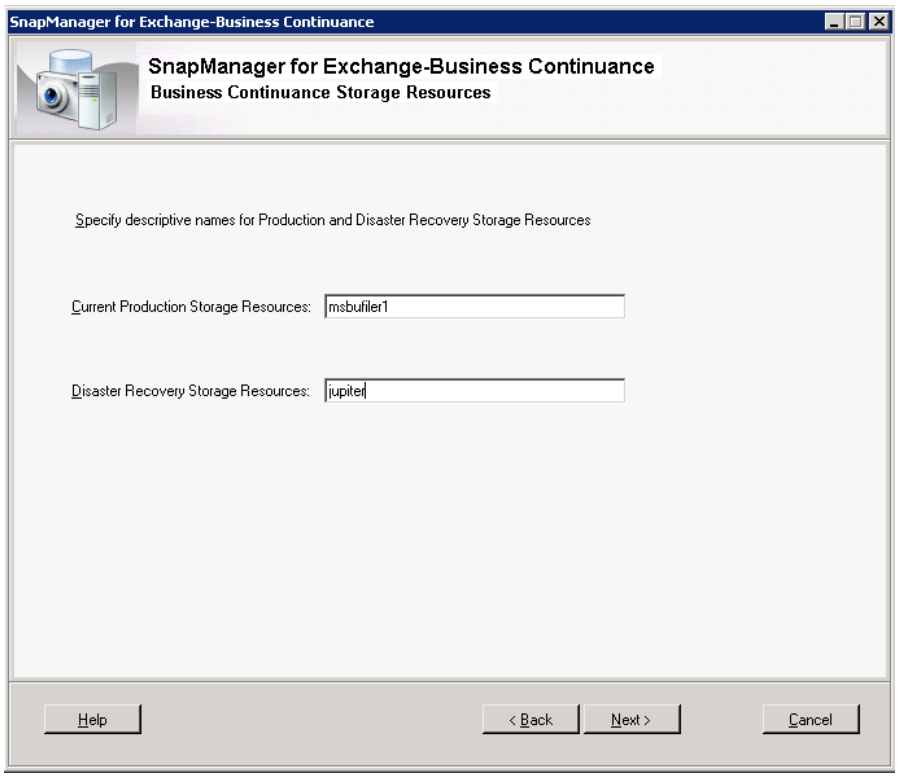


8. Select Choose Existing Resources, Specify Network Name, Resource Group, IP Address, SubNet Mask, and Network type options.

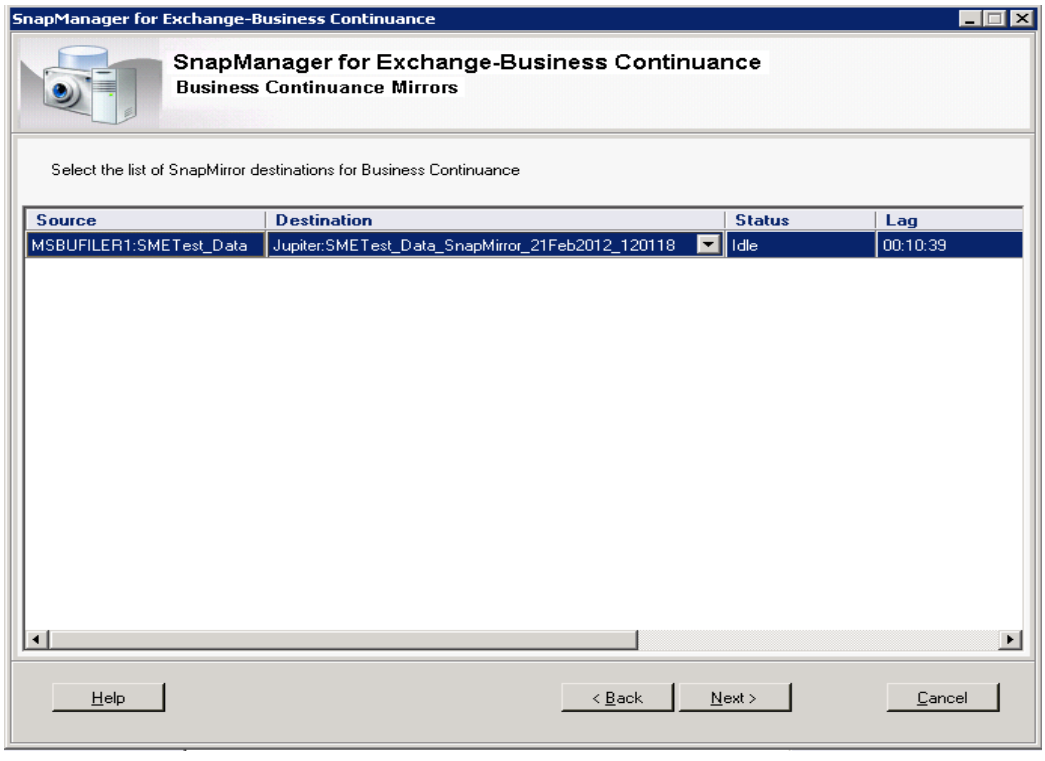




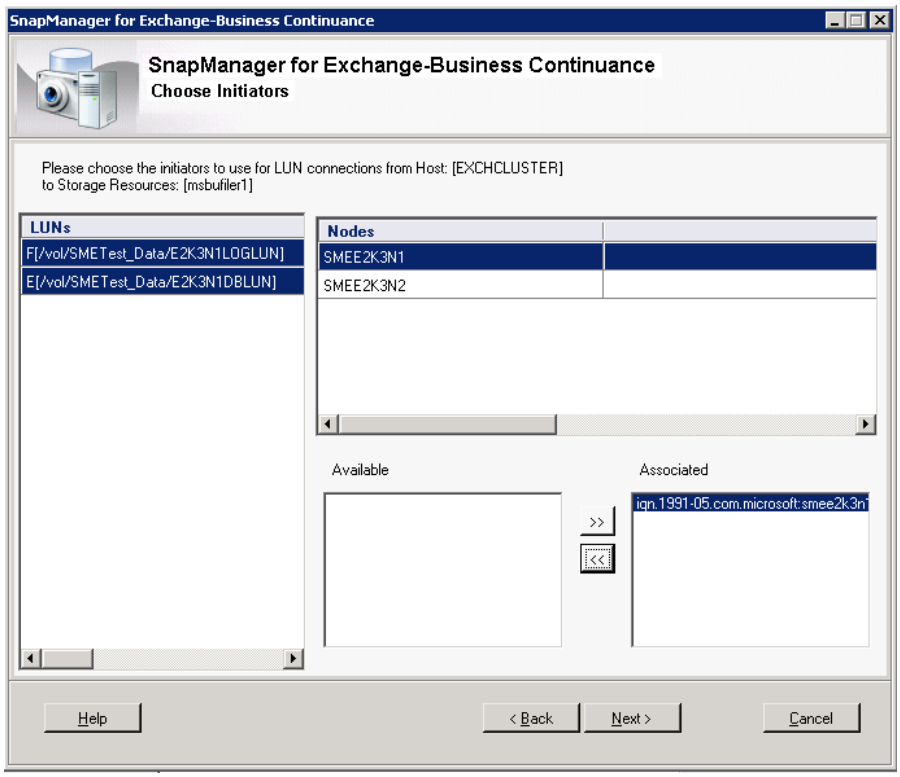
9. In the Business Continuance Storage Resources page, specify the current production storage resources and the storage resources for disaster recovery.

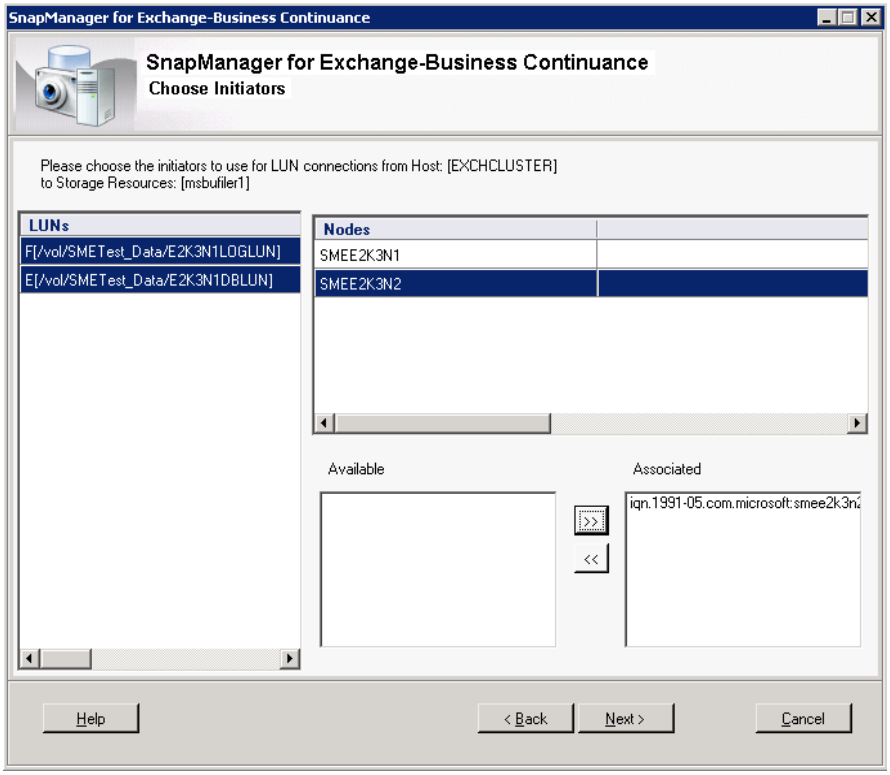


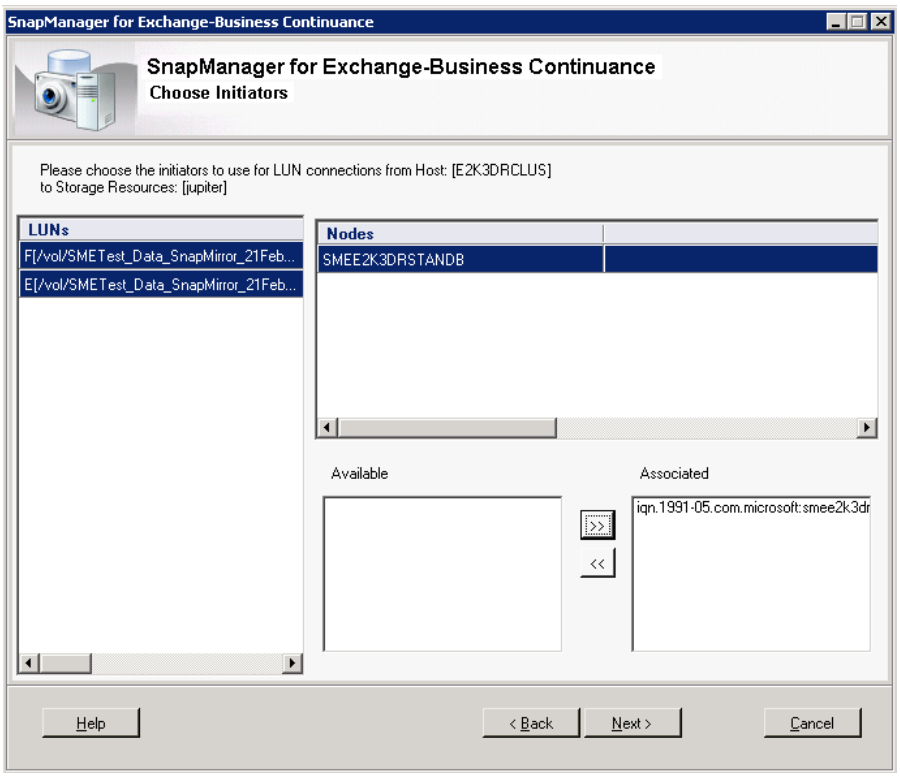
10. In the Business Continuance Mirrors page, select the list of SnapMirror destinations for business continuance.



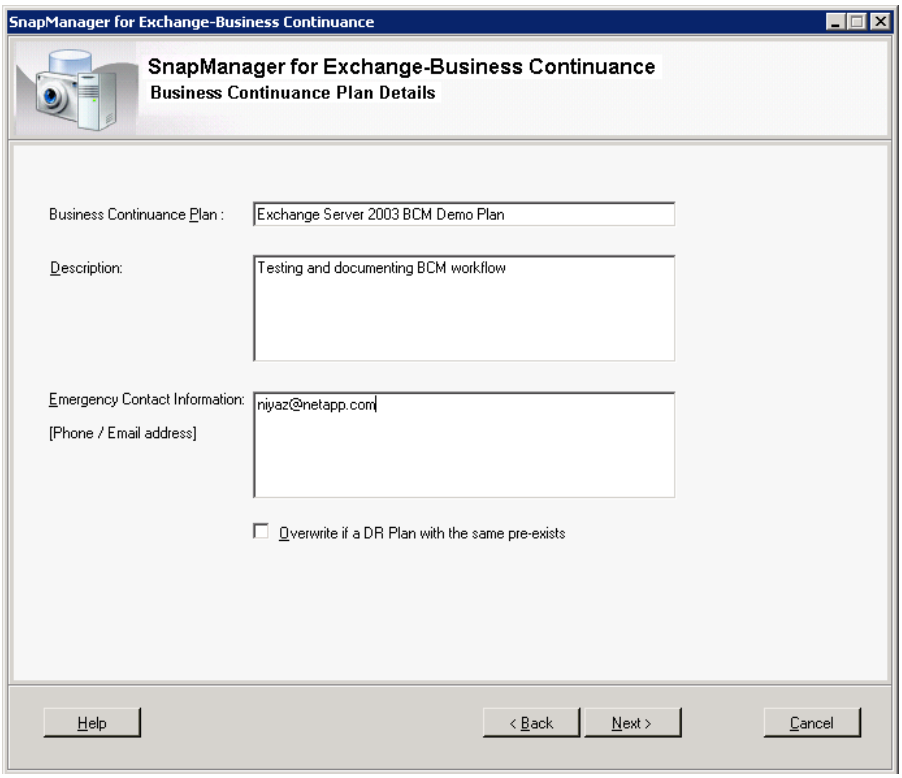
11. In the Choose Initiators page, specify the initiators to use for LUN connections from the host to storage resources.

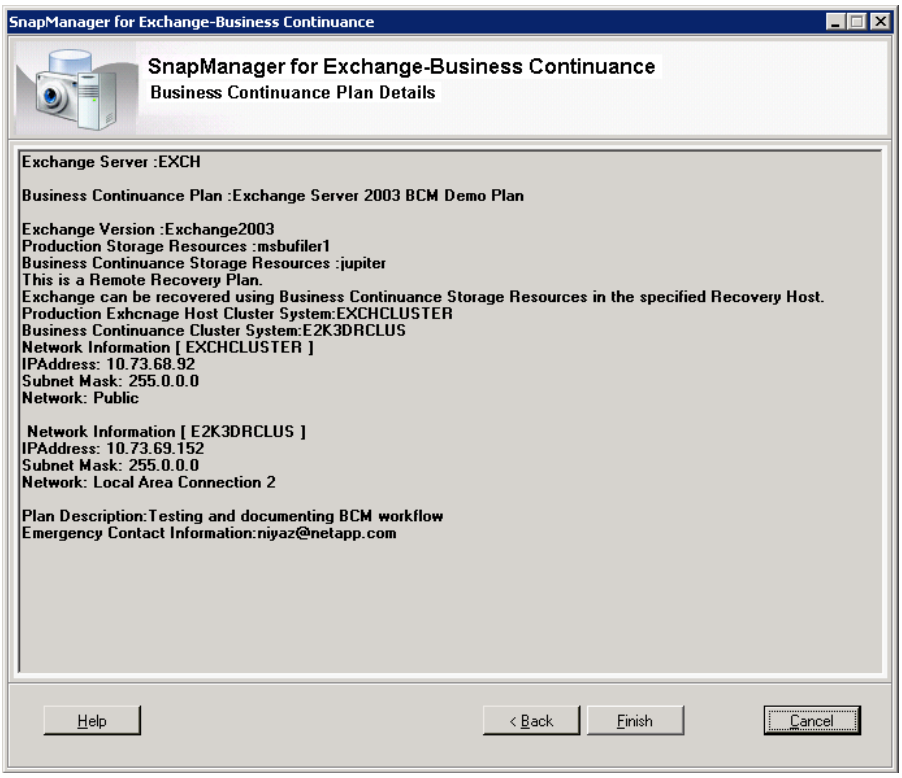




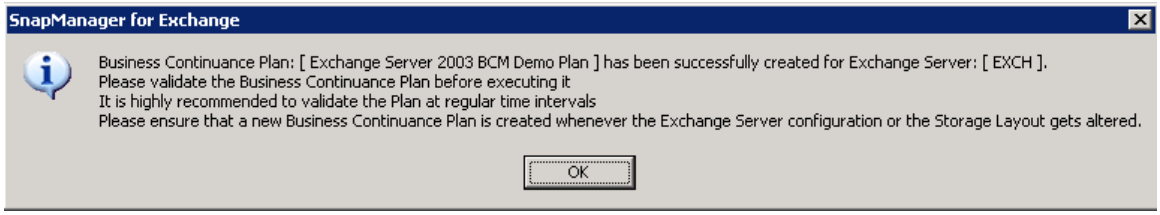


12. In the Business Continuance Plan Details page, specify the name of the business continuance plan, describe the business continuance plan, and provide the emergency contact information.





13. Click Finish > OK > Close.



8 Validating the Business Continuance Plan

You can validate the business continuance plan at any time; however, you should validate it at fixed intervals, especially before starting the failover process. This makes sure the correct resources and server configuration get involved in the recovery operation.

8.1 About This Task

If the mount point root LUNs required for recovery are not a part of the business continuance plan and do not exist on the business continuance host, the business continuance plan validation and execution fail. To avoid such failures, such LUNs should have Exchange or SnapManager SnapInfo directory components in them, and the mount point root drive letters should be created on the business continuance host prior to running the validation.

8.2 Steps

Follow these steps to validate the business continuance plan:

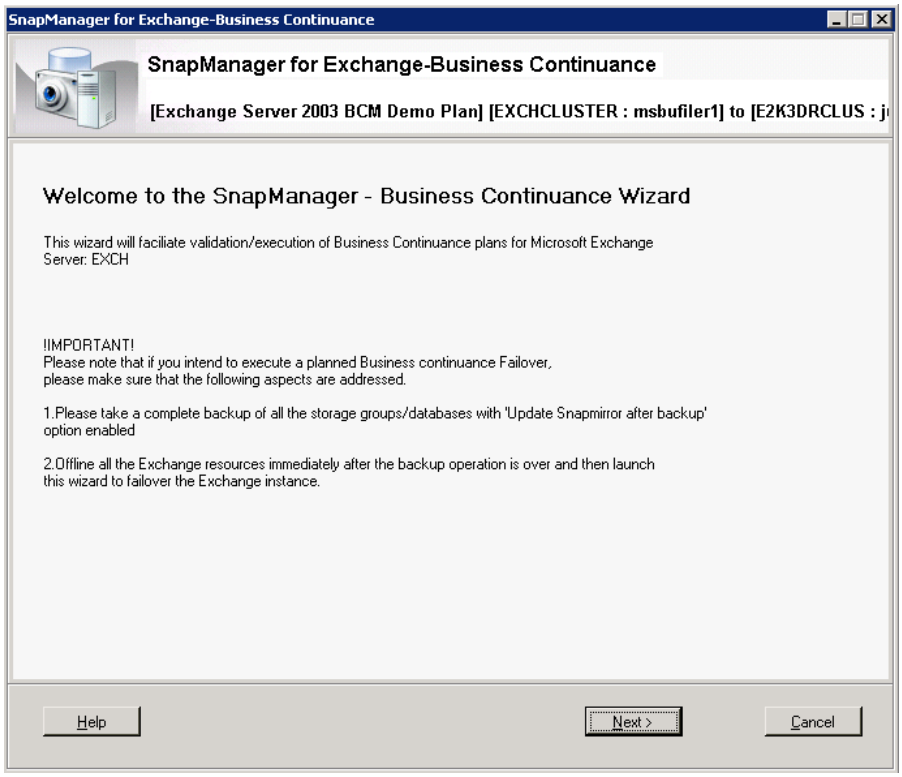
1. Launch the business continuance page using the path Start > All Programs > NetApp >SnapManager for Exchange Business Continuance.

2. In the scope pane, connect to the disaster recovery server to which you want to fail over.
3. In the Actions pane, click Validate.
4. Click Next to confirm the recovery server and the storage resources that you selected for business continuance.
5. Select the Business Continuance activities that need to be performed during execution.
6. Click Finish.
7. In the Status window, click Validate.
8. Click OK.
9. Click Close.

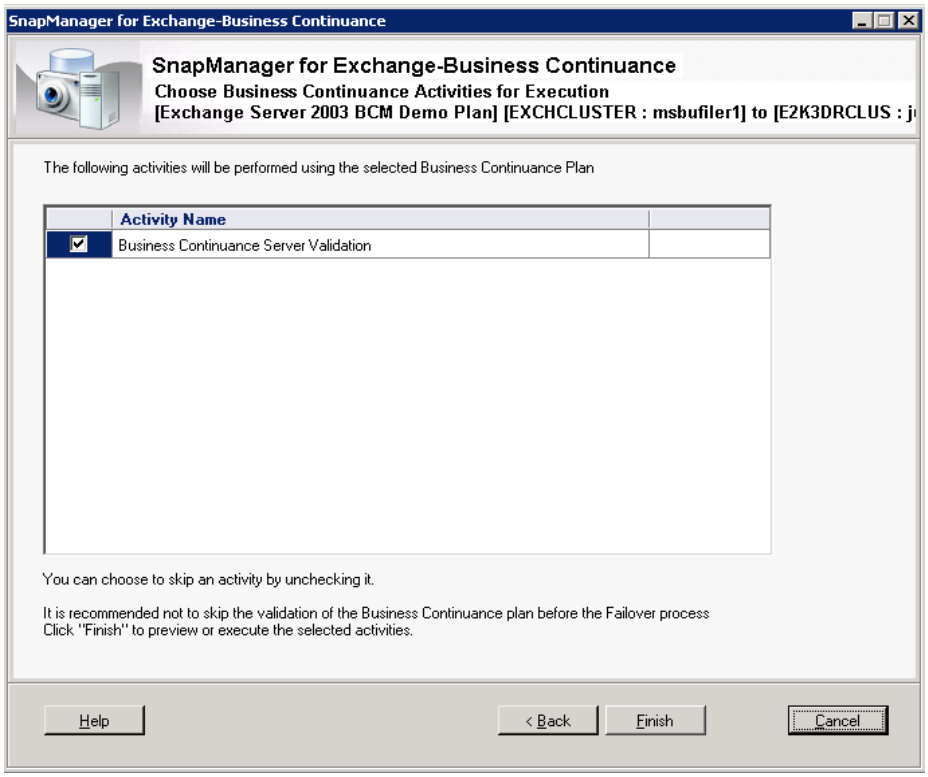
8.3 Validation of Business Continuance Plans for an Exchange Server

The BCM should be configured and validated during periodic intervals so that it can be executed during a test failover or a real disaster.

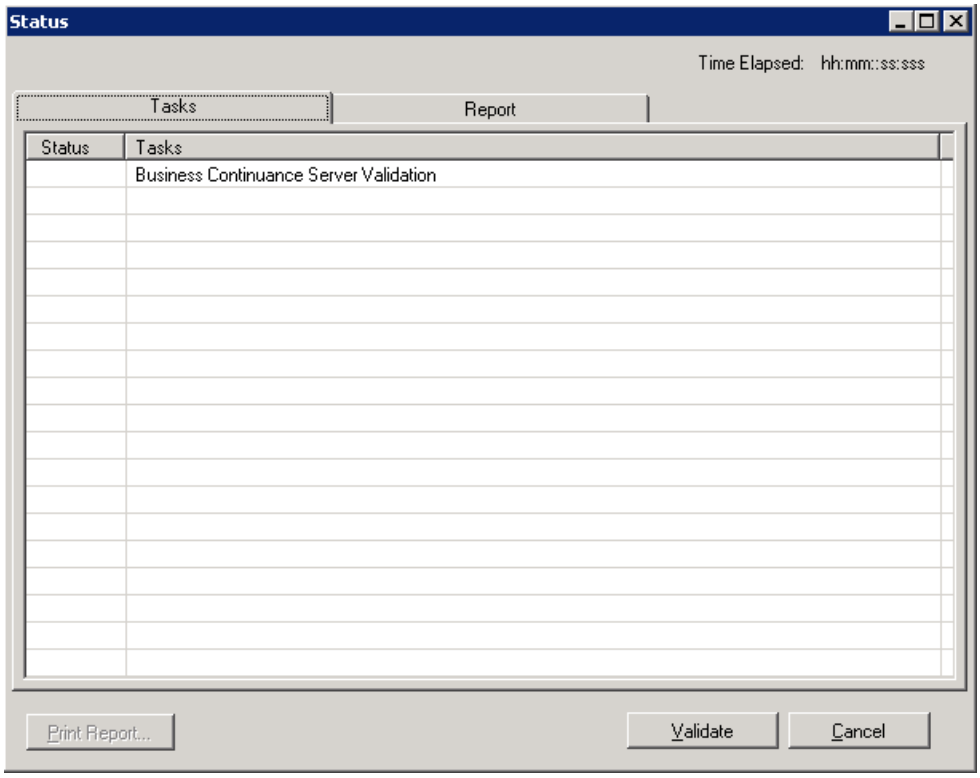
1. Launch the business continuance page using the path Start > All Programs > NetApp >SnapManager for Exchange Business Continuance.
2. In the Actions pane, click Validate.



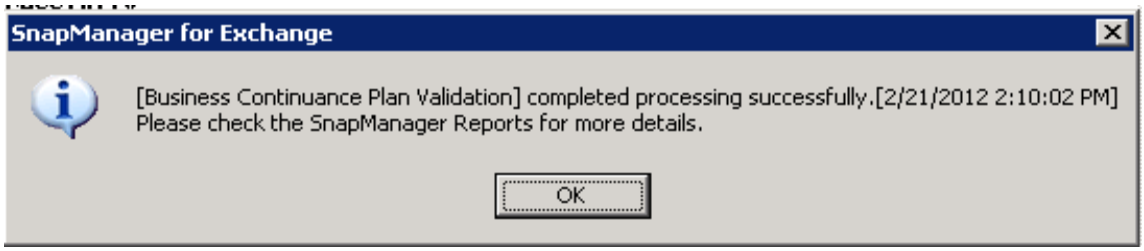
3. Click Next to confirm the recovery server and the storage resources that you selected for business continuance.
4. Select the Business Continuance activities that need to be performed during execution.
5. Click Finish.



6. In the Status window, click Validate.



7. Click OK.



9 Executing the Business Continuance Plan

You can perform the following tasks as part of the business continuance plan: business continuance server validation, cleanup of business continuance destination, take Exchange instances offline, quiesce and break SnapMirror relationships, reconnect Exchange LUNs, Exchange instance recreation, and restore backups.

Best Practices

- If it is a planned failover, be sure to take a complete backup and update the SnapMirror destination.
- Make sure the databases and storage groups do not exist at the destination site for standalone-to-standalone failover. If the Exchange instance is alive (running), SnapManager displays a message to take the Exchange resources offline as part of failover, or it provides an option to exit the wizard.
- Make sure that the mount points or drive letters are available (not in use) at the destination site. For example, if the following are the mount point paths for the source c:\sg1 and c:\logs1, make sure that there is only c:\ at the destination site. The paths will be created by business continuance when it mounts the LUNs. If you are using drive letters F: and T:, they should not be used at the destination as well.
- When the Exchange Server has LUNs that contain mount points, but do not have any Exchange related data on the mount point root LUN, then these LUNs must be created manually prior to the failover to the business continuance site. For example; if LUN "N" has mount point N:\mp on it, then LUN N must be created manually in the business continuance exchange server prior to failover.

9.1 About This Task

As a part of the business continuance plan execution, SnapManager does not restart the Exchange transport service. Mail flow might not resume until you restart the Exchange transport service. You can use the SnapManager replication management console page to fix a SnapMirror relationship error.

9.2 Steps

Follow these steps to execute the business continuance plan:

1. Launch the business continuance plan by using the path Start > All Programs > NetApp > SnapManager for Exchange Business Continuance.
2. In the Scope pane, select the business continuance plan.
3. Connect to the business continuance host in which the Exchange data needs to be recovered.
4. In the Actions pane, click Execute.
5. To revalidate the business continuance plan before executing it, click Yes.
6. In the SnapManager - Business Continuance page, click Next.
7. This step is applicable only for a clustered configuration. In the Business Continuance Plan Details page, select the If the Exchange Instance is alive checkbox to verify whether the Exchange instance is running.
8. In the Business Continuance Plan Details page, click Next.

9. If your Exchange instance is running, take the Exchange resources offline and relaunch the Business Continuance wizard.
10. Click Next> to confirm the recovery server and the storage group that are selected for business continuance.
11. In the Choose Business Continuance Activities for Execution page, select the business continuance activities that need to be performed during execution.

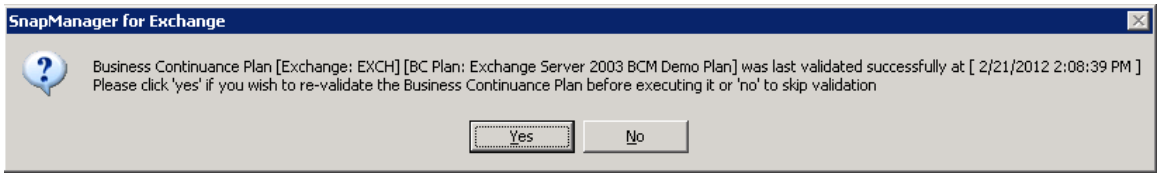
Table 2) Business continuance activities.

If You Want...	Then...
The business continuance plan to be consistent and valid with respect to the current state of Exchange	Select Business Continuance Server Validation.
Make sure that the old production cluster is clean and that there are no failed disk resources	Select Cleanup of Business Continuance Destination. The business continuance cleanup process will not remove the mount point roots, and, in case of Exchange 2007 clusters, it might rename the old resource group, when there are leftover mount point roots.
All of the Exchange storage group instances offline	Select Offline Exchange Instances.
To validate the SnapMirror relationships that are a part of the business continuance plan	Select Quiesce and Break SnapMirror. Any unbroken mirror relationships are broken at this time.
To connect all the LUNs on the SnapMirror destination volume by using the same drive letters	Select Reconnect Exchange LUNs.
To create Exchange cluster resources	Select Exchange Instance Recreation. This step is applicable only for Exchange 2007 and Exchange 2003 cluster-to-cluster configurations. However, the step is skipped automatically for Exchange 2007 standalone configurations.
To execute an up-to-the-minute restore operation or mailbox rehoming	Select Restore backups. If your configuration is Exchange 2007 and 2003, cluster to cluster, SnapManager performs an up-to-the-minute restore operation. If your configuration is Exchange 2007, standalone, SnapManager performs a restore operation with the mailbox rehoming.

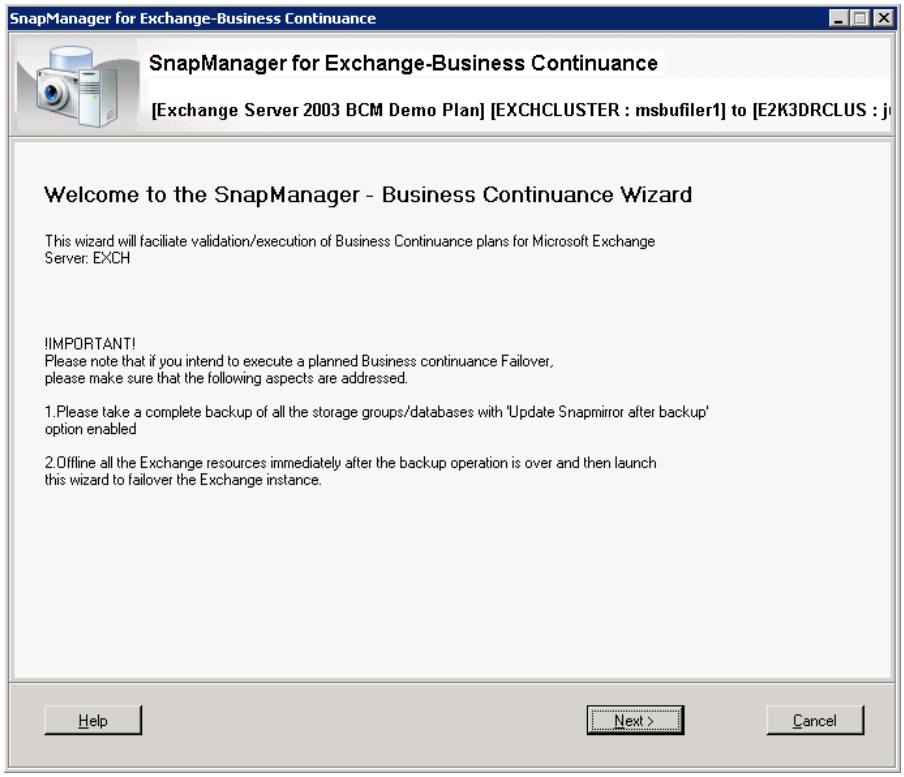
12. Click Finish.
13. In the Status page, click Execute to start the operation.
14. Click OK.
15. In the Status page, click Close.

9.3 Execution of Business Continuance Plans for an Exchange Server

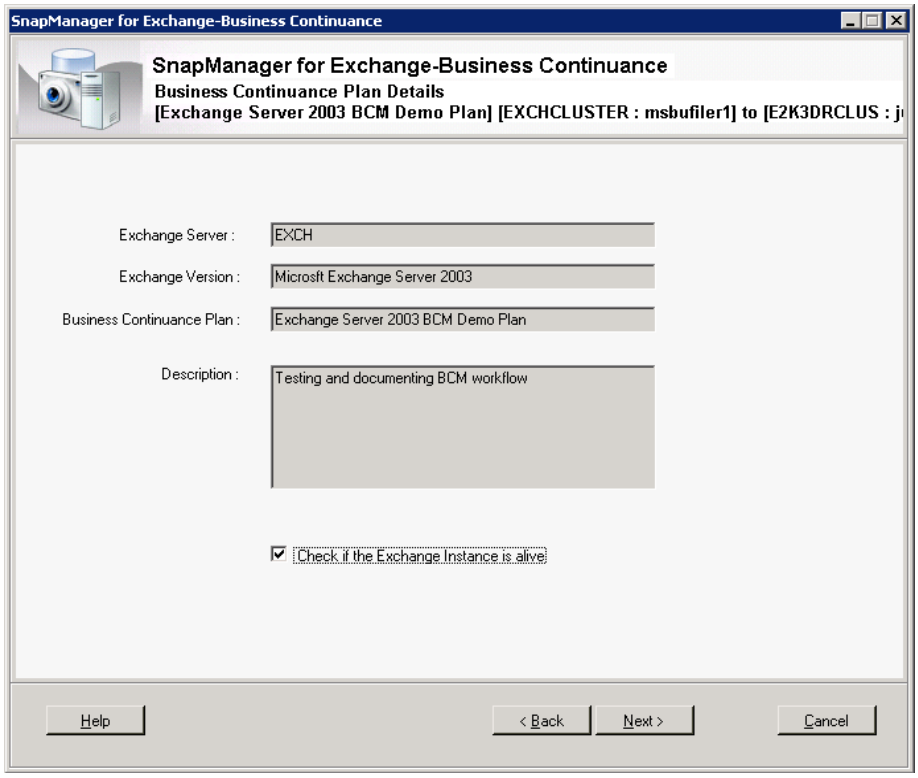
1. To revalidate the business continuance plan before executing it, click Yes.



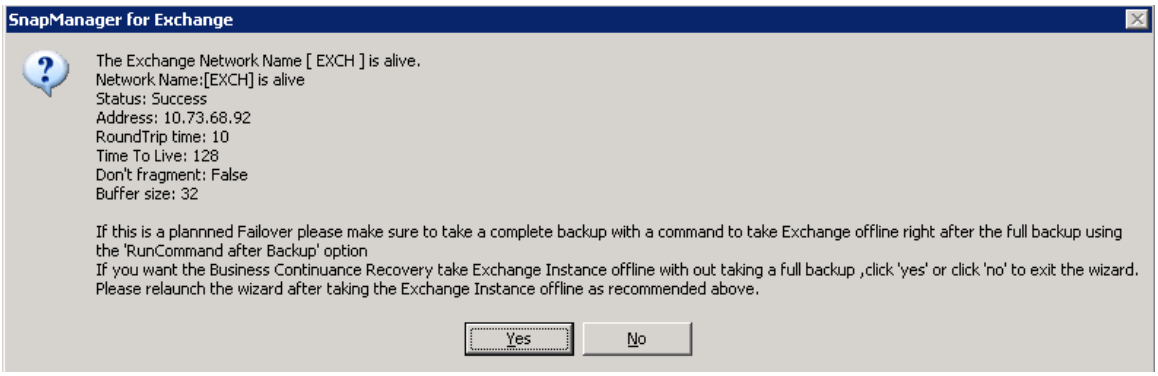
2. In the SnapManager business continuance page, click Next.



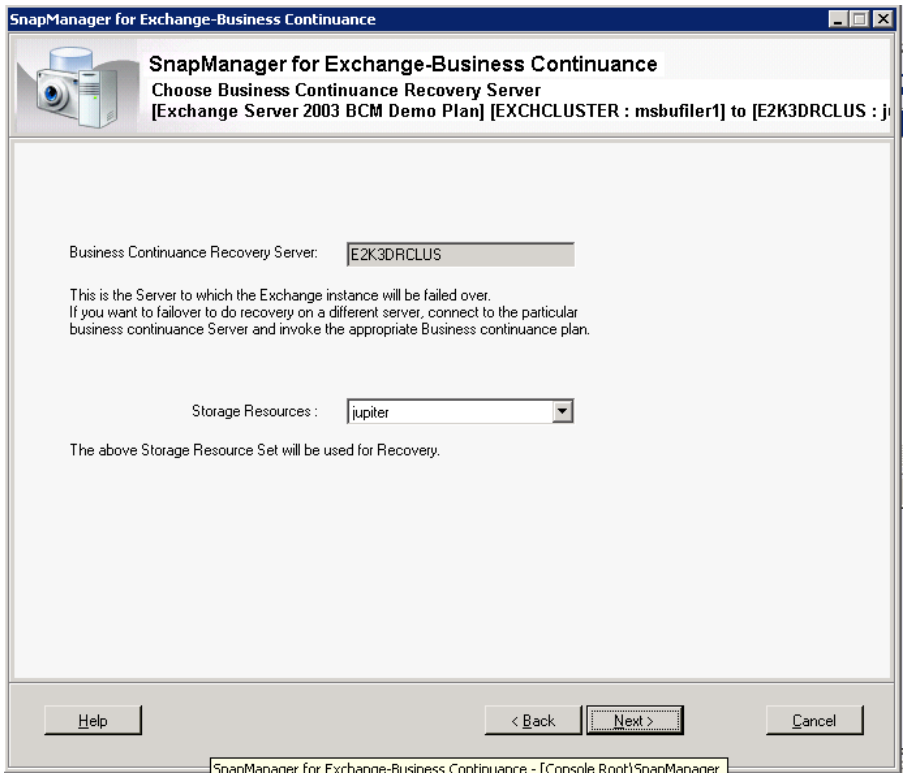
3. This step is applicable only for a clustered configuration. In the Business Continuance Plan Details page, select the If the Exchange Instance is alive checkbox to verify if the Exchange instance is running.



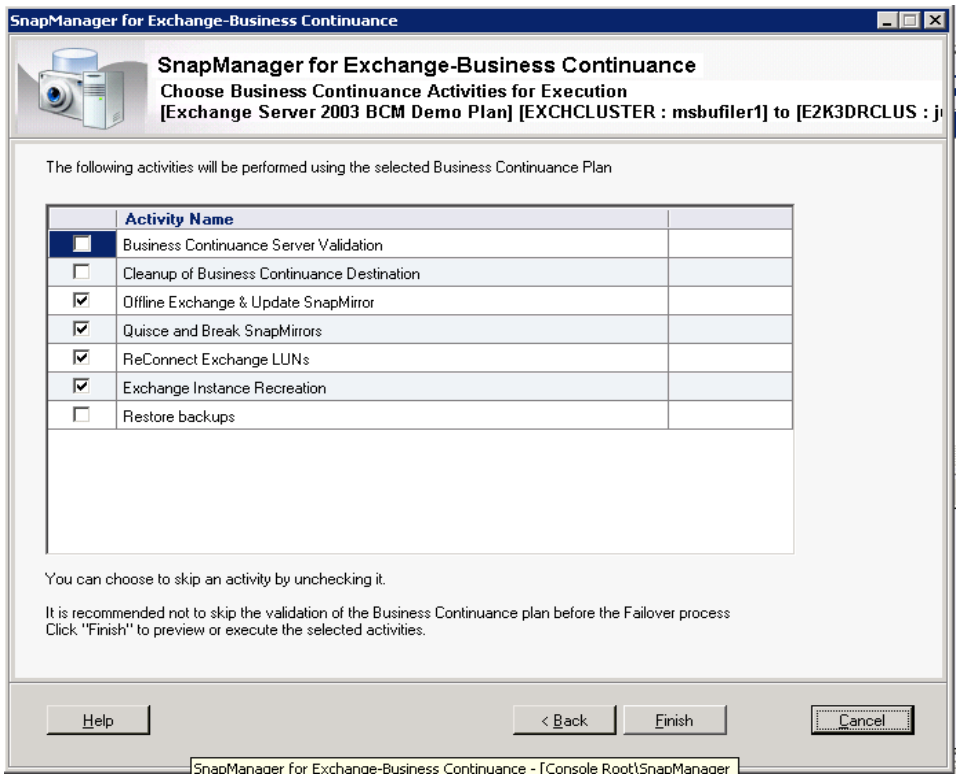
4. In the Business Continuance Plan Details page, click Next.



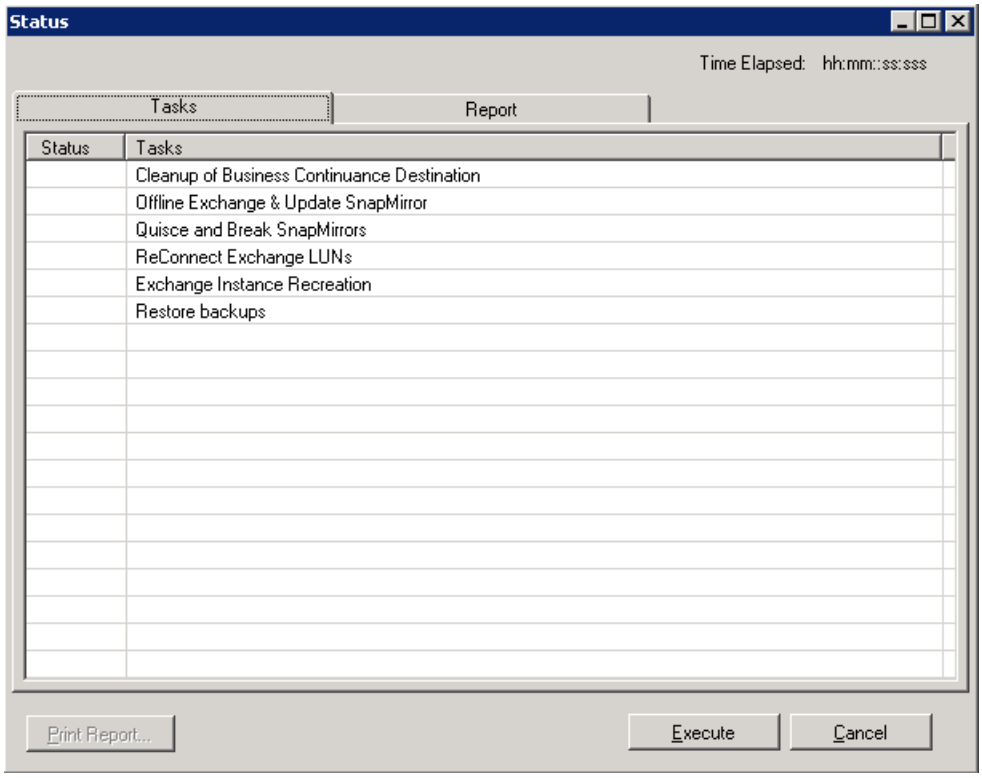
5. Click Next to confirm the recovery server and the storage group that are selected for business continuance.

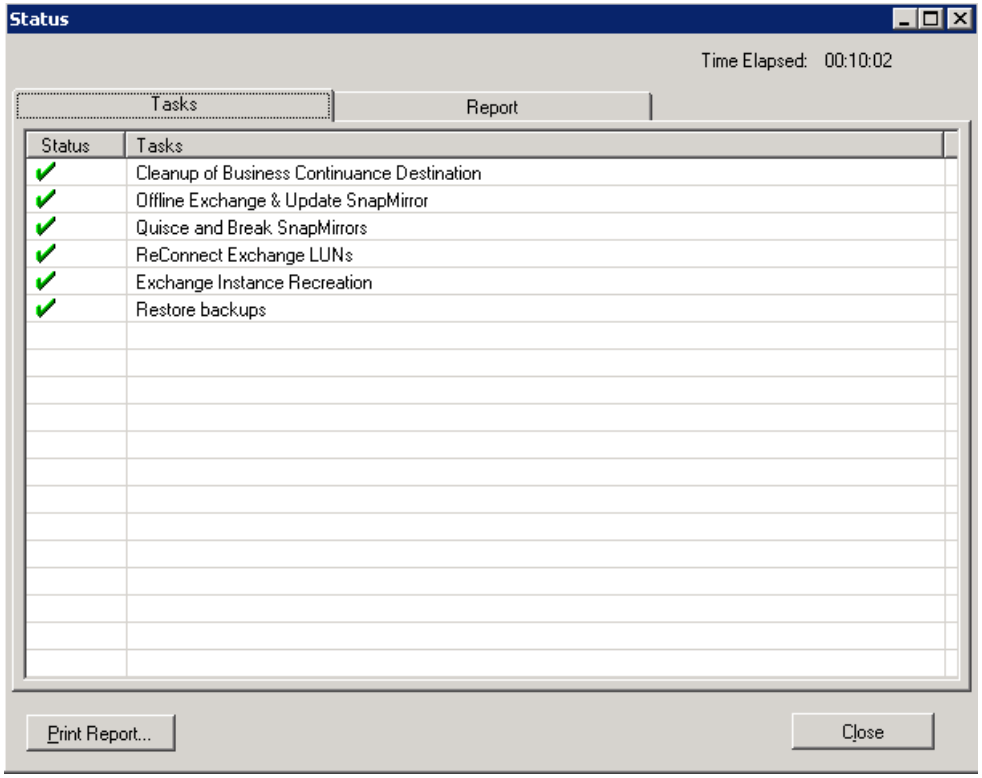


6. In the Choose Business Continuance Activities for Execution page, select the activities that need to be performed during execution.



7. Click Finish.
8. In the Status page, click Execute to continue the operation.





9. Click OK.
10. In the Status page, click Close.

10 Activating SnapManager Business Continuance

For the purpose of this document, Exchange Server 2003 and Exchange Server 2007 are explained as subsections in detail.

10.1 Exchange Server 2003

The SnapManager business continuance offers two kinds of failover mechanisms for Exchange Server 2003.

Storage-Only Failover

Exchange can be recovered using business continuance storage resources in the same host with the help of underlying SnapMirror technology and the destination or local storage resources.

EVS Failover (Recovery of Cluster in Recovery Site)

The standby cluster is used in such scenarios, and the necessary cluster resources will be recreated automatically during the recovery process in the recovery site.

This topic describes how to move the Exchange virtual servers from a production Exchange 2003 cluster using SnapManager for Exchange business continuance to a standby cluster. This process can be used when recovering from the loss of the entire production cluster or as a site resilience solution for Exchange 2003 clusters.

In Exchange 2003 clusters, deleting the system attendant resource does not delete or affect the Active Directory objects associated with the Exchange virtual server. This behavior is used to transfer an Exchange virtual server from a production Exchange 2003 cluster to a standby Exchange 2003 cluster.

Procedure to Install Standby Cluster

1. The node in this cluster is the only node in the standby cluster. It should be installed with the same configuration as the production cluster.

Note: On failover clusters running Windows Server 2003, the single node standby failover cluster would be configured with a local quorum, or a disk quorum can be utilized.

2. Install Windows Server 2003 operating system.
3. Set up the relevant networks.
4. Use the appropriate cluster service account.
5. Configure the standby node using the “create new cluster” action from the “open connection to cluster wizard” window. During this operation, the quorum button can also be used to specify the quorum model.
6. Before installing Exchange 2003 binary files, the MS Distribution Transaction Coordinator (DTC) resource should be created.
7. In Windows 2003, Microsoft recommends installing the DTC as a separate cluster group containing a physical disk, network name, and IP address resource and then adding the MS-DTC resource to the cluster group.
8. Install Exchange binary files.
9. The standby cluster is now ready for use. Install same versions of SnapDrive and SnapManager for Exchange as production servers and create the business continuance plan.

10. Make sure no Exchange virtual server instance is running on the standby cluster.
11. The resource groups and the LUN reconnect are taken care of by the BCM task itself.

The following tasks are performed as part of the business continuance plan: business continuance server validation, cleanup of business continuance destination, take Exchange instances offline, quiesce and break SnapMirror relationships, reconnect Exchange LUNs, Exchange instance recreation, and restore backups.

Exchange Instance Recreation Procedure

1. On the standby cluster, the new Exchange IP address resource is created and brought online.
2. The next step is to create the Exchange network name resource as provided in the BC plan, and the "DNS Registration must succeed" and "Enable Kerberos" checkboxes must be selected.
3. The Exchange network name resource is then bought online.
4. On the standby cluster, the Exchange system attendant resource is created, which will create the other Exchange 2003 cluster resources automatically, and all dependencies are set accordingly.
5. The HTTP/SMTP/POP3/IMAP4 virtual server instances are updated with the new IP address.
6. This step also configures the Exchange 2003 mailbox settings, and the local DNS cache of business continuance host is cleared.
7. With this, the recreation of the Exchange cluster resources is completed successfully.

10.2 Exchange Server 2007

The BCM offers different kinds of failovers for Exchange Server 2007. These include:

Storage-Only Failover

Exchange can be recovered using business continuance storage resources in the same host with the help of underlying SnapMirror technology. However, make sure the databases are dismounted prior to this operation, as the LUNs would be disconnected and reconnected to the new storage system.

Mailbox Rehoming

The database portability in Exchange Server 2007 allows administrators to move a database between servers quickly and easily. Exchange Server 2007 allows the mounting of any database from the same Exchange organization.

This feature may be useful in some disaster recovery scenarios where you want to decrease downtime and get your Exchange functional as soon as possible. This feature is an option in certain disaster recovery scenarios.

Mailbox rehoming uses the move mailbox command with configurationOnly. This command essentially updates the properties of an Active Directory account or mailbox to point it at a new mailbox store.

Before You Begin

- Make sure the databases and storage groups do not exist at the destination site for standalone-to-standalone failover.
- Once the type of failover is determined, which is mailbox rehoming in this case, a series of Windows PowerShell™ cmdlets are run, and a new storage group, along with the respective database, is created. Next, the database must allow itself to be overwritten during a restore operation. The AllowFileRestore is utilized to accomplish this.
- SnapManager will automatically rename the highest generation log available to E0n.log before the recovery. If there are extra log files that need to be recovered, SnapManager performs the following steps as well:

- Do not select "Mount databases automatically after restore."
- After SnapManager restore, manually copy extra log files to Drive:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group_restoredLogs.
- Run Exchange database recovery manually.
- After the database is mounted, the mailboxes homed on the primary database are rehomed to the new server. This is done by running the Get-Mailbox cmdlet and pipelining the output to the Move-Mailbox cmdlet along with the Configurationonly switch.

CMS Failover

The following tasks are performed as part of the business continuance plan: business continuance server validation, cleanup of business continuance destination, take Exchange instances offline, quiesce and break SnapMirror relationships, reconnect Exchange LUNs, Exchange instance recreation, and restore backups.

One of the major functional differences between Exchange 2007 and Exchange 2003 is the /recoverCMS switch in the Exchange setup program.

The /recoverCMS process is used to recover the CMS between nodes. The /recoverCMS process will always recreate resources based on the configuration information in the directory. If databases are added to the primary cluster, the appropriate resources will be populated on the standby cluster when /recoverCMS is run.

During the Exchange instance recreation, BC invokes Exchange 2007 setup.com /recovercms to recover clustered mailbox server instances, and the resources are recreated.

When Exchange 2007 is installed on a cluster (either CCR or SCC), several Exchange 2007 specific resources are created. These include:

- A system attendant resource
- An information store resource
- A database instance resource matching each database created on the CMS

While recreating the resources, the following steps are performed:

1. Navigates to the node that currently owns the Exchange resources.
2. Retrieves the information of the CMS name and CMS IP address from the BC plan.
3. Makes sure the CMS is offline on the source.
4. Locates ExSETUP.exe in Drive:\Program Files\Microsoft\Exchange Server\Bin.
5. Recovers the CMS to the cluster by issuing:

```
setup.com /recoverCMS /cmsName:<CMSName> /cmsIPv4Addresses:<IPAddress>,<IPAddress> or setup.com
/recoverCMS /cmsName:<CMSName> /cmsIPv4Address:<IPAddress>
```

6. By recovering the CMS, all clustered resources are refreshed and recreated.
7. Finally, the local DNS cache of business continuance host is flushed.

Points to Remember

- In Windows 2003, when cluster attempts to create or modify Kerberos-enabled machine accounts, it leverages the rights assigned to the cluster service account. The Windows 2003 cluster service uses this domain account for the logon right at service startup.
- In Windows 2008, when the cluster attempts to create or modify Kerberos-enabled machine accounts, it does so by leveraging the machine account associated with the name of the cluster (this is the cluster name object [CNO]). The Windows 2008 cluster service now starts under “Local System.”

- When the CNO does not have rights to join machine accounts to the domain or modify existing machine accounts, the Exchange setup will fail, after programmatically creating the network name resources and attempting to bring it online.
- This situation most commonly occurs when running:

```
Setup.com /recoverCMS /cmsName:<NAME> /cmsIPv4Address:<IP>
```

- The following errors may be noted during setup where the network name failed to come online due to this issue:

```
Cluster Common Failure Exception: Failed to bring cluster resource Network name (<NAME>) in
cluster group <NAME> online.The group or resource is not in the correct state to perform the
requested operation. (Exception from HRESULT:0x8007139f)
```

- Error 0x8007139f translates to:

  ERROR_INVALID_STATE
- The group or resource is not in the correct state to perform the requested operation.

Setting Permissions for Business Continuance on Windows 2008

Follow these steps to set permissions for BC on Windows 2008:

1. Display the Active Directory Computers and Users window.
2. From the View menu, choose Advanced Features.
3. Navigate to the computer's container and select the computer account for the CMS name.
4. Right-click the account name and select Properties.
5. Click the Security tab.
6. Make sure you have selected the computer's object type. Click Add.
7. Click OK to save your changes.

   The system displays the Select Users, Computers, or Groups dialog box.
8. Enter the cluster management name of the disaster recovery cluster and click Check Names.

   The system displays the Properties window again with your cluster management name highlighted.
9. Click all of the Allow checkboxes in the Permissions pane to give full control permissions to the cluster management name.
10. Click OK to save your changes.
11. Open the DNS record.
12. Select the forward lookup zone for the domain and then select the record for the CMS.
13. Right-click the record and select Properties.
14. Click the Security tab.
15. Make sure you have selected the computer's object type and then click Add.
16. Click OK to save your changes.

    The system displays the Select Users, Computers, or Groups dialog box.
17. Enter the cluster management name of the disaster recovery cluster and then click Check Names. The system displays the Properties window again with your cluster management name highlighted.
18. Click all of the Allow checkboxes in the Permissions pane to give full control permissions to the cluster management name.
19. Click OK to save your changes.

11 Failing Back to the Production Site

The failback procedure is similar to the failover procedure except for the SnapMirror resynchronization operation. You can perform a failback using the same disaster recovery plan only if the mirrors are resynchronized in the reverse direction to the original production storage resources. You can also create a new disaster recovery plan to fail over the Exchange storage resources to the production site.

Depending on the state of the production site, the following methods can be utilized:

- **Failing back to the production site (primary storage intact)**

  You can perform a failback using the same disaster recovery plan only if the mirrors are resynchronized in the reverse direction to the original production storage resources using the replication management console or system manager. Here the primary storage is intact, and a resync operation can be used to reverse the SnapMirror relationship.

  Note: Make sure previous Exchange disks in the destination are disconnected or removed before the resync operation is executed.

- **Failing back to the production site (primary storage destroyed)**

  You can also create a new disaster recovery plan to fail over the Exchange storage resources to the production site.

  Note: If new SnapMirror relationships need to be configured in a reverse direction, create and initialize the SnapMirror relationships, from the FilerView® or storage system console or System Manager, and create a new BC plan.

Here, the primary site is destroyed, and the production cluster needs to be rebuilt. Later reconnect the necessary storage controllers, making sure the resources are presented to the cluster. Install the Exchange and the necessary service packs and hotfixes on all the nodes and configure the main site. Follow the same methodology explained in the section Creating a Business Continuance Plan and execute it.

Before you start a planned failback operation from the business continuance site, execute the business continuance plan cleanup task, start reverse resynchronization from the destination to the source storage system, and flush the local DNS cache by following these steps:

1. If you have a clustered configuration and already have a production site where you performed business continuance, execute the business continuance plan cleanup task to remove the remaining Exchange resources and to disconnect the old LUNs.
2. Perform this cleanup before you resynchronize the mirrors in the reverse direction.
3. From the replication management console, initiate reverse resynchronization from the destination storage system to the source storage system.
4. Verify that the SnapMirror relationship is in a state from which a transfer can take place.
5. Flush out the local DNS cache and delete the stale entries after the failover process.
6. After failover\failback from the business continuance site, you might need to update the new IP in a reverse lookup zone of DNS.
7. The local DNS cache in the business continuance site (all of the nodes of the business continuance cluster for a clustered configuration), are flushed automatically as a part of the recovery operation. If the IP address is different in the disaster recovery site, the automatic flush enables connection to SnapManager from the business continuance server after a recovery operation without a manual removal of the local DNS cache.
8. Make sure that each SnapMirror alias is unique in its system and that there is no other invalid, stale, or old destination volume relationship for the same destination volume.
9. To remove any prior history, run setup.com /clearlocalcms /cmsname:<> on the destination cluster.

   Note: The cleanup task also performs clearlocalcms automatically.

10. Make sure that any LUN clone split operation that is in progress is completed.
11. To check that any LUN clone split operations are complete, use the storage system's LUN clone split status command or view the operation status column in the SnapDrive Microsoft management console (MMC).
12. The LUN clone split functionality, introduced in Data ONTAP 7.1, supports significantly faster online Snapshot copy restore times when using SnapManager or SnapDrive to restore database. By default, this functionality is enabled.

    Note: If you attempt a failback procedure immediately after a failover that uses a LUN clone split (such as a test of a failover and failback), the LUN clone split operation might interfere with SnapMirror during resynchronization with the data back to the production site.

11.1 Procedure for Failing Back to the Production Site

You can perform a failback using a disaster recovery plan only if the destination volumes are resynchronized in the reverse direction to the original production storage resources. You can also create a new disaster recovery plan to fail over the Exchange storage resources to the production site.

Before You Begin

Make sure you meet all the prerequisites mentioned in the document before you start the failback process.

Steps

Follow these steps to start the failback process:

1. Launch the replication management console.
2. Click Business Continuance (DR: PROD).
3. Select the destination volumes.
4. If there are no SnapMirror relationships, create new destination volumes through storage system commands and initialize them.
5. Click Sync to resynchronize the destination volumes in the reverse direction if they are broken.
6. Create a final backup of all the storage groups at the business continuance site with a destination volume update of all LUNs.
7. Connect to the production host.
8. Select the disaster recovery plan.
9. In the Actions pane, click Execute.
10. In the dialog box that appears, either click Yes to validate the business continuance plan before executing it or continue without validation.
11. In the SnapManager - Business Continuance window, click Next.
12. This step is applicable only for Exchange Server 2003 or Exchange Server 2007 clustered configuration to make sure that the clustered mailbox server or Exchange virtual server is not running. In the business continuance plan details window that appears, make sure that the Exchange instance checkbox is selected to verify that the Exchange instance is running.
13. In the Business Continuance Plan Details window, click Next.
14. If the Exchange instance is not running, SnapManager displays a message that the network name is not alive, along with complete error details. If the Exchange instance is running, SnapManager displays two options, one to take the Exchange resources offline as part of failover, and the other to exit the wizard, to take the Exchange resources offline, and then relaunch the wizard.

15. In the Choose Business Continuance Recovery Server page, click Next to confirm the recovery server and the storage group that are selected for business continuance.
16. In the Choose Business Continuance Activities for Execution page, select the business continuance activities that need to be performed during execution.

Table 3) Business continuance activities for execution.

If You Want...	Then...
The business continuance plan to be consistent and valid with respect to the current state of Exchange	Select Business Continuance Server Validation.
The old production cluster to be clean and has no failed disk resources	Select Cleanup of Business Continuance Destination.
All of the Exchange storage group instances offline	Select Offline Exchange Instances.
To validate the SnapMirror relationships that are a part of the business continuance plan	Select quiesce and break SnapMirror relationships. Any unbroken mirror relationships are broken at this time.
To connect all the LUNs on the SnapMirror destination volume by using the same drive letters	Select Reconnect Exchange LUNs.
To create Exchange cluster resources	Select Exchange Instance Recreation. This step is applicable only for Exchange 2007 and Exchange 2003 cluster-to-cluster configurations. However, the step is skipped automatically for Exchange 2007 standalone-to-standalone configurations.
To execute an up-to-the-minute restore operation or mailbox rehoming	Select Restore backups. If your configuration is Exchange 2007 and 2003, cluster to cluster, SnapManager performs an up-to-the-minute restore operation. If your configuration is Exchange 2007, standalone to standalone, SnapManager performs a restore operation with the mailbox rehoming.

17. Click Finish.
18. In the Status page, click Execute to start the operation.
19. Click OK.
20. In the Status page, click Close.

After You Finish

Perform a release operation on reverse mirrors after you fail back.

12 Managing SnapMirror Replication

You can manage the SnapMirror replication of Exchange volumes across the production site and business continuance site using the replication management console by following these steps:

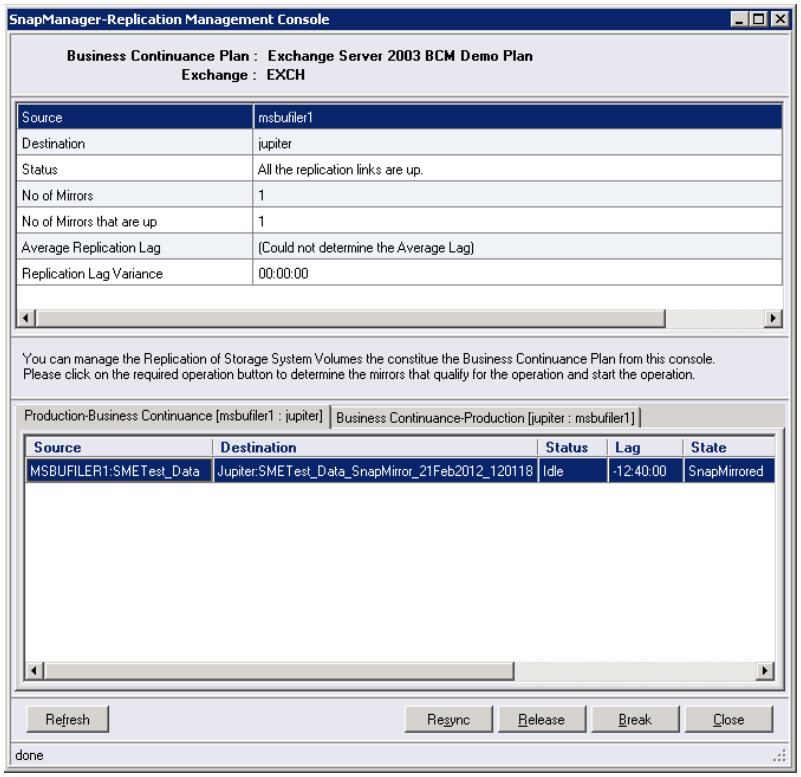
1. In the Actions pane, click Replication Management.

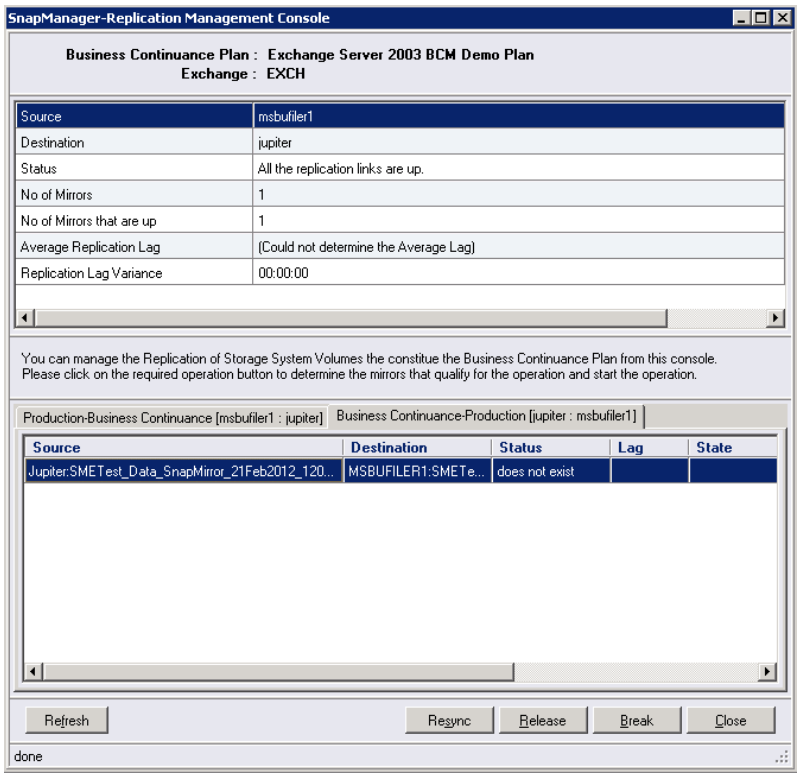
Table 4) Replication management console.

If You Want To...	Then...
Synchronize the SnapMirror relationship between the source and the destination storage systems	Click Sync and then select the SnapMirror relationships that you want to resynchronize, release, or break.
Release the SnapMirror relationship established between the source and the destination storage systems	Click Release.
Break the SnapMirror relationship established between the source and the destination storage systems	Click Break.

2. Click Start.

   The replication management console displays the progress of the SnapMirror synchronization, release, or break operations.





13 Troubleshooting

SnapManager reports list details of every SnapManager operation that you perform, their final status, and any error messages that you encounter during the operation.

The SnapManager BC report directory provides folders that group the reports for each of these operation types:

- Business continuance
- Debug

Alternatively, collect the Windows event logs, SDW debug logs, storage system message logs, and the nSanity tool to gather more data and contact NetApp Support for assistance.

Viewing SnapManager Reports

You can view SnapManager reports from the SnapManager GUI by following these steps:

1. In the Scope pane, click Reports.

   SnapManager displays the report folders in the Results pane.
2. In the report folders, select the database for which you want to view a report.

   SnapManager displays the report in the Results pane.

14 Summary

Microsoft Exchange is a mission-critical application, and it can cripple the operational productivity in case of downtime or unavailability. NetApp has proven data protection and disaster recovery tools for Microsoft Exchange. SnapManager for Exchange backup and restore capabilities, combined with SnapDrive and

SnapMirror technologies, provide a solid and robust solution for protecting and recovering your Exchange data, while meeting stringent RPOs and RTOs based on your business requirements.

References

Here is a list of Microsoft resources on the Web that were referenced in this document.

- Cluster IP Resource Fails with Event ID 1048 After Network Change
  http://support.microsoft.com/kb/267548
- The clustered MSDTC resource fails when you change the PDC Emulator operations master role to a different node in the cluster on a computer that is running Windows Server 2003
  http://support.microsoft.com/kb/900216
- Events are logged after an IP address change on an Exchange cluster
  http://support.microsoft.com/?kbid=315691
- How To: Create a New Zone on a DNS Server in Windows Server 2003
  http://support.microsoft.com/kb/323445
- Changing the IP address of network adapters in cluster server
  http://support.microsoft.com/kb/230356
- Permissions recommended for the CNO (Cluster Name Object) in Windows 2008 for Exchange 2007 SP1 setup operations
  http://blogs.technet.com/b/timmcmic/archive/2009/02/24/permissions-required-for-the-cno-cluster-name-object-in-windows-2008-for-exchange-2007-sp1-setup-operations.aspx
- Microsoft Exchange 2003
  - How to Move All Exchange Virtual Servers from a Production Exchange 2003 Cluster to a Standby Exchange 2003 Cluster
    http://technet.microsoft.com/en-us/library/aa996470(EXCHG.65).aspx
  - Exchange 2003 Disaster Recovery Operations Guide
    http://technet.microsoft.com/en-us/library/bb125070(v=exchg.65).aspx
  - Activating Standby Continuous Replication Targets
    http://technet.microsoft.com/en-us/library/bb691321(v=exchg.80).aspx
- Microsoft Exchange 2007
  - Standby Continuous Replication
    http://technet.microsoft.com/en-us/library/bb676502.aspx
  - High Availability
    http://technet.microsoft.com/en-us/library/bb124721(v=exchg.80).aspx
  - TR-3578: Microsoft Exchange Server 2007 Best Practices Guide
    http://media.netapp.com/documents/tr-3578.pdf
- Data ONTAP 8
  https://support.netapp.com/documentation/productlibrary/index.html?productID=30092
- SnapManager for Exchange
  - SnapManager for Microsoft Exchange Server
    https://support.netapp.com/documentation/productlibrary/index.html?productID=30034
  - TR-3845: SnapManager 6.0 for Microsoft Exchange Best Practices Guide
    http://media.netapp.com/documents/tr-3845.pdfSnapDrive for Windows
- SnapDrive for Windows
  - SnapDrive for Windows
    https://support.netapp.com/documentation/productlibrary/index.html?productID=30049
  - TR-3828: SnapDrive 6.2 for Windows Best Practices
    http://media.netapp.com/documents/tr-3828.pdf

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

www.netapp.com