Technical Report

Microsoft Exchange Server and SnapManager for Exchange Deployment Guide

Niyaz Mohamed, NetApp
April 2014 | TR-4280

Executive Summary

This deployment guide assists customers in deploying solutions as per best practices to meet specific business requirements. It is based on the experiences of existing NetApp customers, real-world simulations, and NetApp engineering lab validations. The deployment guide helps customers through the entire project lifecycle, including requirement assessment, solution design, installation, and administration.

Note: This guide specifically focuses on NetApp® clustered Data ONTAP® deployment scenarios.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1   E-Mail Business Requirements

Electronic communication and e-mail services have shifted from a convenience to a critical business tool supporting the most important business processes, such as sales and customer service. Additionally, e-mail messages, including file attachments, often contain sensitive or confidential business information, and the Microsoft® Exchange database is often the sole repository of this information. Dependence on e-mail for business communications makes it one of the most mission-critical applications in a company. Any interruption to e-mail services can have an immediate impact on daily operations. The longer a service disruption lasts, the more significant is the impact. A day of downtime can have a major negative impact on the entire business, with the potential for unrecoverable losses in the sales and customer service divisions.

Along with increased reliance on e-mail service, businesses also are seeing an increase in the amount of information stored in their e-mail databases. This increase in database size is a result of continued growth in the number of messages sent and received, as well the size of e-mail attachments and embedded images. To meet their business needs, companies are seeking a messaging backbone with a resilient architecture that is easy to manage and maintain and that provides high availability. Additionally, the e-mail service must be cost effective, because it is only one of the many priorities in the IT department. These two requirements—high availability and cost effectiveness—challenge many IT leaders. The solution presented in this document answers these challenges.

2   Solution Deployment Details

This section discusses the details of the various components used in the solution; outlines the preparation, installation, and configuration of these components; and offers operational guidance.

The section begins by discussing the roles of Microsoft Exchange server followed by the NetApp storage layout used by Microsoft Exchange server. It also highlights the solution components and the overall architecture.

2.1   Microsoft Exchange Server Roles

Unlike earlier versions, Microsoft Exchange server 2013 includes only two server roles:

- **Client access servers (CASs)**. All client traffic connects to the now stateless CAS server. For more information about the Microsoft Exchange 2013 client access server role, see Client Access Server on Microsoft TechNet: http://technet.microsoft.com/en-us/library/dd298114%28v=exchg.150%29.aspx.
- **Mailbox servers**. These servers maintain mailbox store databases, client access protocols, transport service, and unified messaging components. For more information about the Microsoft Exchange 2013 mailbox server role, refer to Mailbox Server on Microsoft TechNet: http://technet.microsoft.com/en-us/library/jj150491%28v=exchg.150%29.aspx.

2.2   Storage Environment

NetApp FAS Storage Controllers

The NetApp FAS series is the storage platform used in this solution. This platform offers the following advantages for this solution.

- Clustered Data ONTAP allows two or more controllers (or nodes) to operate as one shared resource pool or storage cluster. The storage cluster can be expanded, contracted, and subdivided nondisruptively into one or more secure partitions, or Storage Virtual Machines (SVMs). An SVM is a logical storage container that includes allocated storage resources from within the cluster as well as security parameters such as rights and permissions.

- Capacity management features provide the ability to grow as demands on the e-mail service increase.
- Integration of the layers of storage, Microsoft Windows®, and Microsoft Exchange simplify and automate data backup and restoration.
- Various levels of data protection meet the high-availability requirements of the e-mail service.

2.3   Additional NetApp Software Used

Table 1 lists the additional NetApp software used.

Table 1) Additional NetApp software used.

Name	Description
Data ONTAP	Clustered Data ONTAP operating system
SnapDrive® for Windows	Storage provisioning
SnapManager® for Exchange	Backup and recovery
Single Mailbox Recovery	Single-item recovery

The solution presented in this deployment guide not only meets business requirements, but it offers additional benefits compared to other solutions that use a standard direct-attached storage implementation or a similar SAN implementation. This section describes how the solution meets the requirements stated earlier, and discusses the additional benefits as well.

Figure 1 illustrates the method for configuring solution components for both the primary and secondary sites.

Figure 1) Method for configuring solution components for both the primary and secondary sites.
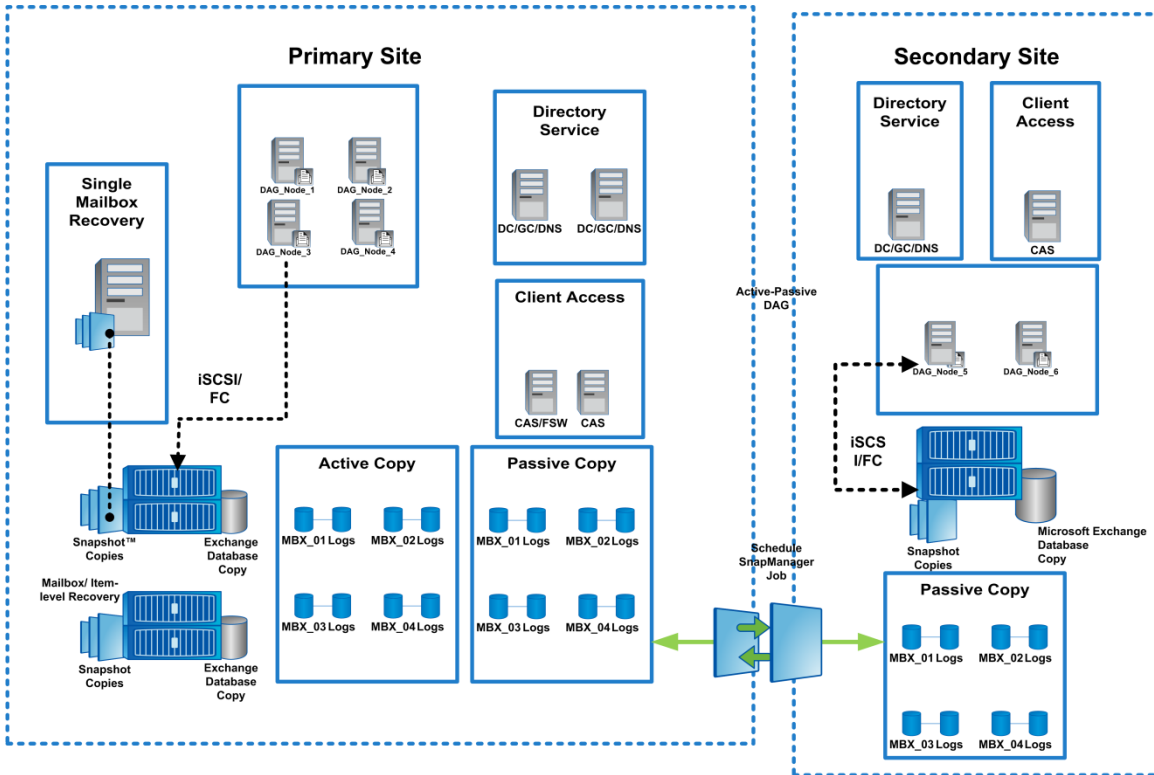
Virtualization

Server virtualization is a major component of data center virtualization and plays a key role in the virtualization initiative. NetApp has been on the forefront of solving complex business problems with its innovative technology breakthroughs and end-to-end solutions approach. The virtualization platform, through its ability to virtualize Microsoft Exchange, assists in efficient use of hardware resources that can be combined with the other key advantages of server virtualization, which include better availability, lower cost, and increased flexibility. You can realize multiple benefits from using Microsoft Exchange in a virtualized environment with NetApp storage technology, including:

- **Effective use of server hardware**. Migrating the entire Microsoft Exchange environment from dedicated physical servers that have relatively low utilization rates can lead to significantly higher server utilization.
- **Consolidation**. Small and medium-sized organizations, as well as remote offices for larger organizations, deploy the Exchange Server roles into a virtualized platform with other application servers on the same physical server.
- **Savings**. You save on power and space.
- **Reduced server hardware requirements**. The number of physical servers required to support Microsoft Exchange can also be reduced.

    Note: When virtualizing Exchange 2013 roles, NetApp recommends that these roles be separated onto different host servers. In the event of a host server failure, this separation prevents failure of any particular role. For example, deploying one Client Access Server (CAS) and two mailbox servers per host server provides a good mix in terms of distribution of roles.

    Note: SnapManager for Exchange is qualified with guest initiator LUNs and pass-through disks in Hyper-V® environments. In VMware® environments, SnapManager for Exchange is validated with guest initiator LUNs (easy for deployment) and iSCSI/FC RDMs.

Database Storage Layout Planning

Let us look at an example of the customer requirements used in this guide for layout design.

- 10,000 2GB mailboxes—100 messages per day (75KB)
- DAG with 2 database copies in the primary data center and 1 database copy in the secondary site
- 1 week (7 days) of online Snapshot™ copies and 3 days of log retention
- 2TB database size

The storage layout is designed to meet capacity and I/O requirements along with the backup requirements, which would be handled by SnapManager for Exchange. SnapManager for Exchange requires that the transaction logs and database files be placed on separate flexible volumes.

Table 2 lists the storage layout format.

Table 2) Storage layout format.

Component	Description
FlexVol® volumes	1 for each database, 1 for each log
LUNs	1 for each database, 1 for each log

**Note:** We assume that the transaction logs are placed on separate volumes and LUNs in this specific example. The transaction logs for multiple databases can also be placed in a single volume.

For the most current information about storage system volume and LUN planning, refer to TR-4221: Microsoft Exchange Server 2013 and SnapManager for Exchange Best Practices Guide for Clustered Data ONTAP.

2.4   Disk Layout

Figure 2 illustrates the disk layout scheme required to meet the I/O and capacity requirements of the SLA.

Figure 2) Disk layout scheme required to meet the I/O and capacity requirements of the SLA.
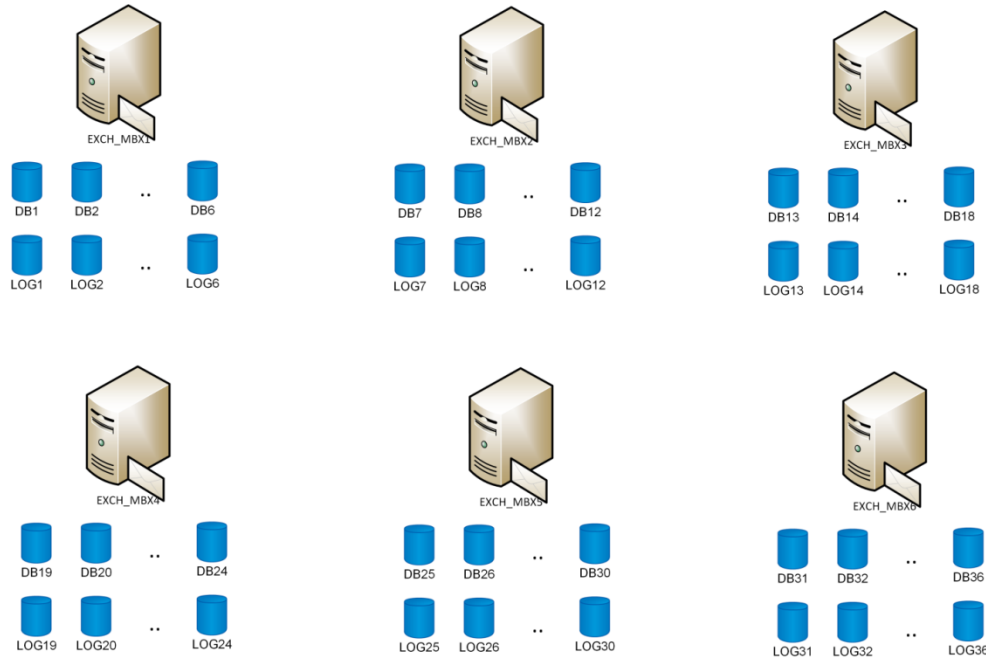
Volume and LUN Layout Recommendations

Data ONTAP enables the creation of flexible volumes for managing data without the need to assign physical disks to the volumes. Instead, the FlexVol volumes enjoy performance benefits from a larger pool of physical disks called an aggregate.

Using FlexVol volumes results in the following benefits for Microsoft Exchange environments:

- Using FlexVol volumes, the capacity and performance bandwidth of a large collection of fast drives can be made available to all volumes. Even very small FlexVol volumes have the performance benefit of very large number of drives.
- A large number of volumes can be created, all with independent Snapshot copy schedules, mirroring policies, and so on.
- All volumes can be managed independently while receiving the maximum I/O benefit of a much larger pool of disks.

When considering Microsoft Exchange 2013 LUN configurations, the number of LUNs you provision largely depends on the recovery point objectives (RPOs) and the recovery time objectives (RTOs).

The Microsoft Exchange database and transaction log files should be separated onto separate LUNs and separate volumes. This allows greater flexibility for backup and recovery procedures and data protection strategies. For example:

- /vol/db1_vol/db1_lun.lun ----> db1.edb
- /vol/log1_vol/log1_lun.lun ----> e00xxxx.log
- /vol/db2_vol/db2_lun.lun ----> db2.edb
- /vol/log2_vol/log2_lun.lun ----> e01xxxx.log

and so on.

As with databases, place the transaction logs and SnapInfo for each database into separate volumes. Although the logs and SnapInfo for the same Microsoft Exchange database should be put into the same volume, the logs and SnapInfo for separate Microsoft Exchange databases should be put into different volumes. This layout results in the best combination of storage capacity use, performance, and restore options.

When creating the LUNs to hold Microsoft Exchange data, use mountpoints rather than drive letters. For failover purposes in a DAG configuration, the path for every database copy (the active database and all passive copies) must be the same on each of the DAG member servers. But although each copy of the database should be the same across the servers in the DAG, each database path and transaction log path must be unique per database. Microsoft Exchange environments that require multiple databases can quickly use the available drive letters for a given server. When there are no available drive letters to assign to a LUN, use volume mountpoints (VMPs). VMPs are directories on a Windows volume that map to a mounted LUN. VMPs can be used at any time, whether drive letters are available or not. Note that not all drive letters are eliminated. A minimum of one drive letter remains mapped to a LUN that serves as the volume mountpoint root.

Another best practice is to put databases (and transaction logs) from different servers into separate volumes. If databases from multiple servers are stored in the same volume, then while a Snapshot copy is being created based on the backup schedule for one server, a successful Snapshot copy cannot be created based on the backup schedule of another server. In this scenario, Snapshot copy schedules can "overlap" for different servers whose databases share a volume. Using a separate volume for databases from each server reduces complexity and eliminates the possibility of copy schedules overlapping.

Determine how many LUNs are required for SnapManager configuration and what data those LUNs hold. Then create a data configuration plan by calculating the required sizes for each LUN and the volume that contains it.

Note: If Microsoft Exchange databases reside on a LUN, do not add mountpoints to that LUN. If you have to complete a restore of a database residing on a LUN with volume mountpoints, the restore operation removes any mountpoints that were created after the backup, disrupting access to the data on the mounted volumes referenced by these volume mountpoints.

As mentioned earlier, each copy of a database must be located at the same path on every mailbox server that holds a copy of the database. Each FlexVol volume should be configured as follows.

- Automatic Snapshot copies are disabled.
- The Snap Reserve is set to 0% (snap reserve 0).
- **The fractional reserve is set to 0% (vol options <volname> fractional_reserve 0)**. No additional space is reserved from the volume for overwrites to LUNs. The storage system will only show the volume of data written to the LUN, plus data in the volume held in Snapshot copies.
- **LUN space_reservation is disabled**. This means that no space is preallocated from the volume at the point that the LUN is created. The storage system will show used space increasing because the data is written to the LUN.
- The volume will be thin provisioned (vol options guarantee =none).
- **Deduplication is enabled.** Each of the database FlexVol volumes in the environment is configured with deduplication enabled. Because the LUNs are not space reserved and the FlexVol volumes are not space guaranteed, any blocks freed up by the dedupe process will be returned to the free space in the aggregate.

The benefits of configuring the storage as described in the preceding section is as follows.

- The configuration allows space reporting (df) to show more accurately the space that is consumed in the aggregate because volume guarantee=none, fractional reserve is 0%, and LUN space reservation is disabled.

- There is no requirement to provision initial volume sizes with a large space overhead for Snapshot copies because volume autogrow adds additional space to the volume as required.
- Space for Snapshot copies in the aggregate is thin provisioned by using autosize. A large free space pool in the aggregate means that individual volumes can have their autogrow maximum size set larger than if autogrow were not implemented.
- The `aggr show_space` command shows the total allocated and the total used for all volumes in the aggregate so you can find out exactly how much space is consumed in the aggregate.

2.5   Volume Sizing

Volume sizing is broken into two different parts:

- Database volume sizing
- Transaction log volume sizing

NetApp recommends that when sizing Microsoft Exchange volumes, the Microsoft sizing spreadsheet for Microsoft Exchange first be used to determine the appropriate amount of space needed for each LUN. Total volume requirements (Database Volume Space Required and Log Volume Space Required) are used as the basis for calculating volume space requirements.

Transaction Log Volume Sizing

Providing accurate sizing for transaction log volumes depends on the following factors.

- Total transaction log LUN size: The total size of all transaction log LUNs that will be stored in one transaction log volume
- Snapshot copy space: The space consumed by transaction logs generated during a 24-hour period

Transaction log volume sizing can be calculated using the following formula.

Transaction log volume size = Total transaction log LUN size + (Snapshot copy space * online backup retention duration)

Provided that an accurate change rate is known, the following formula can be used to calculate total volume size. To calculate the Microsoft Exchange DB volume size, use the following variables:

- **Database LUN size**. The size of the LUN used to store the Microsoft Exchange mailbox database
- **Database daily change rate**. The amount the Microsoft Exchange mailbox database changes in a day, expressed as a percentage of the database size
- **Online backup retention duration**. The number of days that backups are kept online; a day is measured by 24 hours

Database volume size can be calculated using the following formula:

Database volume size = (Sum of the database LUN sizes that will share the database volume) + ([fault tolerance window + online backup retention duration] * database daily change rate)

Based on the volume sizing formula, Table 3 lists the volume size for one database and log, respectively.

Table 3) Volume size per database and log.

Volume Type	Volume Purpose	Volume Size	Total Number of Volumes
Transaction logs and SnapInfo	Transaction logs and SnapInfo	188GB	36
Database	Database	2842GB	36

The volume requirements for each server should be placed onto different nodes of the NetApp cluster; this will spread the load and provide a resilient solution. The active and passive copies of the databases can be placed on separate aggregates that are part of separate Storage Virtual Machines (SVMs) to provide higher availability from storage perspective.

2.6 Installation and Configuration

This section provides an overview of the installation sequence, as well as specific configuration parameters, with a focus on the NetApp solution components.

Table 4 describes the primary tasks to install and configure the solution.

Table 4) Installation and configuration procedure.

Steps	Task	Description
1.	Review the solution design	• Review and sign off on the requirements and design • Make sure that business objectives and IT deliverables are aligned
2.	Prepare data centers	• Rack space and power preparations • Cabling, network ports, and SAN ports • TCP/IP address and DNS host names **Note:** The power supply requirements are relevant to the hardware that is used. For information about power supply requirements specific to the customer environment, refer to the appropriate technical specification documentation. **Note:** For detailed information about the site preparation requirements, see the NetApp Site Requirements Guide.
3.	Install server hardware	• Install server hardware • Comply with both internal standards and hardware vendor best practices
4.	Install and configure FAS storage arrays	• Physical installation • Install clustered Data ONTAP • Create aggregates with RAID-DP and volumes as per the recommendation and best practices from NetApp **Note:** RAID-DP is a high-performance implementation of RAID 6 that provides double parity across the disk subsystem and protects against the failure of up to two disks per RAID group. Calculations have shown double parity RAID offers over 160 times the protection against data loss than RAID 10 does and almost 4,000 times the protection against data loss than RAID 5.
5.	Prepare and validate Microsoft Active Directory® environment	• Prepare Active Directory prerequisites for Microsoft Exchange 2013

Steps	Task	Description
6.	Install and configure Microsoft Windows for Exchange servers	Update prerequisites for Microsoft Exchange 2013 **Note:** The full installation option of Windows Server® 2008 R2 with SP1, Windows Server 2012 or Windows 2012 R2 must be used for all servers that run Exchange 2013 server roles. **Note:** The computer running the Exchange 2013 server roles must be joined to the appropriate Active Directory forest and domain.
7.	Install and configure Microsoft Exchange roles	• Install mailbox server and the Client Server roles • Create DAG • Configure transport settings and Client Access
8.	Install NetApp SnapDrive on Exchange mailbox servers	• Install SnapDrive prerequisites • Install SnapDrive software on all nodes of DAG and provision LUNs from FAS controller
9.	Install and configure online Exchange backups	• SnapManager for Exchange installation on all the nodes of DAG • Frequent Recovery Point configuration • Single Mailbox Recovery installation on designated mailbox servers or dedicated server • Configure and schedule backups
10.	Test and validate the solution	• Pretest of solution readiness • Fault-tolerance test and validation – Refer to Appendix B • Validation of backup and restore – Refer to Appendix B

For detailed installation and configuration steps, refer to **Appendix A: "Installation and Configuration Details**" in this guide.

Installing NetApp SnapDrive on Microsoft Exchange Mailbox Servers

The Microsoft Exchange 2013 mailbox server role depends heavily on storage for a stable and reliable configuration. NetApp offers many advantages over other storage vendors for Microsoft Exchange, most notably the ability to capture the state of the Microsoft Exchange 2013 databases at various points in time, called Snapshot copies. These Snapshot copies are taken in coordination with the Microsoft Exchange 2013 VSS engine. The NetApp SnapDrive and SnapManager for Exchange products provide the underlying host intelligence required to present storage over the supported storage protocol and to coordinate Microsoft Exchange 2013–aware backups. As a result, NetApp SnapDrive software should be installed before any involved configuration of Exchange databases has occurred.

NetApp SnapManager for Exchange does allow the migration of Exchange 2013 databases to NetApp storage after configuration. Consequently, the following instructions for installing and configuring NetApp SnapDrive precede the Microsoft Exchange 2013 database configuration instructions.

Preparations for Installing SnapDrive

Before setup begins, verify the compatibility of all hardware and software involved using the NetApp Interoperability Matrix Tool.

Prepare each Windows Host part of the Microsoft Exchange DAG in the SnapDrive configuration.

1. Verify that the host meets the minimum requirements for use with SnapDrive.
2. Determine whether the Microsoft iSCSI Software Initiator program is installed.
3. Determine whether SnapDrive was previously installed.
4. Determine which FC or iSCSI HBA or MPI/O components are already installed.

SnapDrive supports three protocols for creating and managing LUNs: iSCSI, FC, and FCoE. Before installing SnapDrive for Windows, install or upgrade the relevant components on the host computer.

Table 5 lists the required components.

Table 5) Required components.

Scenario	Tasks
The iSCSI protocol and software initiator will be used to create and manage LUNs.	• Install or upgrade the Microsoft iSCSI Software Initiator. • Install the iSCSI host utilities on the hosts. • NetApp highly recommends installing Data ONTAP DSM for multipathing.
The iSCSI protocol and hardware initiator will be used to create and manage LUNs.	• Install the iSCSI HBA. • Upgrade or install the iSCSI HBA driver and firmware. • NetApp highly recommends installing Data ONTAP DSM for Multipathing. Install the iSCSI host utilities on the hosts if Data ONTAP DSM is not installed.
The FC protocol will be used to create and manage LUNs.	• Install FCP HBA or CNA for FCOE. • Upgrade or install the FC driver and firmware. • NetApp highly recommends installing Data ONTAP DSM for Multipathing. Install the Windows host utilities on the hosts if Data ONTAP DSM is not installed.

Prepare Each Storage System in SnapDrive Configuration

1. After verifying that licenses for FC, iSCSI, or both are enabled on the storage system, start the services by entering the `fcp start` command or the `iscsi start` command at the storage system command line.

   Note: For more information, refer to the appropriate "Data ONTAP Administration Guide" on the NetApp Support site.

2. Prepare volumes as per the planned layout on the storage system to hold SnapDrive LUNs.

SnapDrive Prerequisites in Clustered Data ONTAP Environments

Before installing SnapDrive for Windows, the following prerequisites must be met.

Table 6 lists the prerequisites prior to installing SnapDrive for Windows.

Table 6) Prerequisites prior to installing SnapDrive for Windows.

Description of Prerequisites
The following licenses are required on the storage system: • Fibre Channel Protocol (FCP) or iSCSI (depending on the configuration) - Use FC/iSCSI-accessed LUNs. • FlexClone® technology - Enables volume clone functionality on flexible volumes. • SnapRestore® technology - Restore LUNs from Snapshot copies. • SnapDrive / SnapManager_Suite (either on the host or on the system) - Use whichever license enables SnapDrive functionality when the SDW license is not on the host. • SnapVault® technology (optional). • SnapMirror® technology (optional). To determine which licenses are enabled on a storage system, complete these steps: 　1. Log in to the storage system through the console or telnet. 　2. Type `license` to display the list of licenses installed. **Note:** This can also be done through System Manager.
A SnapDrive user service account on the storage system is required. **Note:** This account is required to connect SnapDrive to the storage system.
The transport protocol (HTTP, HTTPS, or RPC) that SnapDrive will use to communicate with the storage system must be determined. **Note:** NetApp recommends using HTTPS. The HTTPS protocol allows using the Data ONTAP interface for all interactions between the storage system and the host, including sending passwords securely. For SnapDrive to use the HTTP or HTTPS protocol, the `httpd.admin.enable` option must be set on the storage system. **Note:** The RPC protocol is not supported by SnapDrive on clustered Data ONTAP systems.
NET Framework 4.0 is required.
NetApp Windows Host Utilities 6.0.2 or later is required.
The required hotfix for Windows 2012 is 2859162 and for Windows 2008 R2 the hotfixes are 2522766, 2528357, 2494016, 2520235, 2531907, and 974930.
An SVM with the following settings and configurations is required: • Data volumes with junction paths defined • SVM management LIF with the following parameter settings: `data=role, protocols=none, firewall policy=management` • Vsadmin password is set and the account is unlocked • On each node in the cluster, a data LIF for SAN protocols that is separate from any data LIFs

Note: Set appropriate storage controller options for the volume.

Note: Synchronize the storage controller clocks with the Active Directory servers and configure DNS settings on the storage controller. Verify that name resolution is working before installing SnapDrive for Windows on the hosts.

Install and Configure Online Exchange Backups

Installing SnapManager for Exchange for Online Backups

Download the SnapManager for Exchange software from http://support.netapp.com/ and follow the installation steps.

For detailed installation steps, refer to **Appendix A: "Installation and Configuration Details**" in this guide.

Prior to installing SnapManager for Exchange, make sure the prerequisites are followed and met.

Table 7 lists the prerequisites prior to installing SnapManager for Exchange.

Table 7) Prerequisites prior to installing SnapManager for Exchange.

Description of Prerequisites
The following components must be installed or configured on the storage system. • iSCSI or Fibre Channel (FC) protocols • SnapManager license • SnapRestore license • SnapMirror license • FlexClone license
The SnapDrive preferred IP address (if the storage system has multiple IP addresses), Microsoft iSCSI Software Initiator, and SnapDrive for Windows must be installed.
Storage must be configured and the LUNs must be presented to the Windows servers.
SnapManager for Exchange Server (SME) runs as a service on Windows servers and requires a service account. The SME service account must be the same on all of the servers in a DAG environment and must be part of the **Organization Management role** in Exchange. Effectively, the SME account has Org Level access in Microsoft Exchange.

NetApp SnapManager Database Migration/Configuration

After installation of SnapManager for Exchange, complete the following steps to migrate the databases to NetApp LUNs and to configure the Snapinfo folder for the backup metadata.

1. Log in to the designated node as the user Domain\SMEuser and start SnapManager for Exchange.
2. Select an Exchange server or a DAG server to connect to. In this example, SMEXCHDAG is selected.
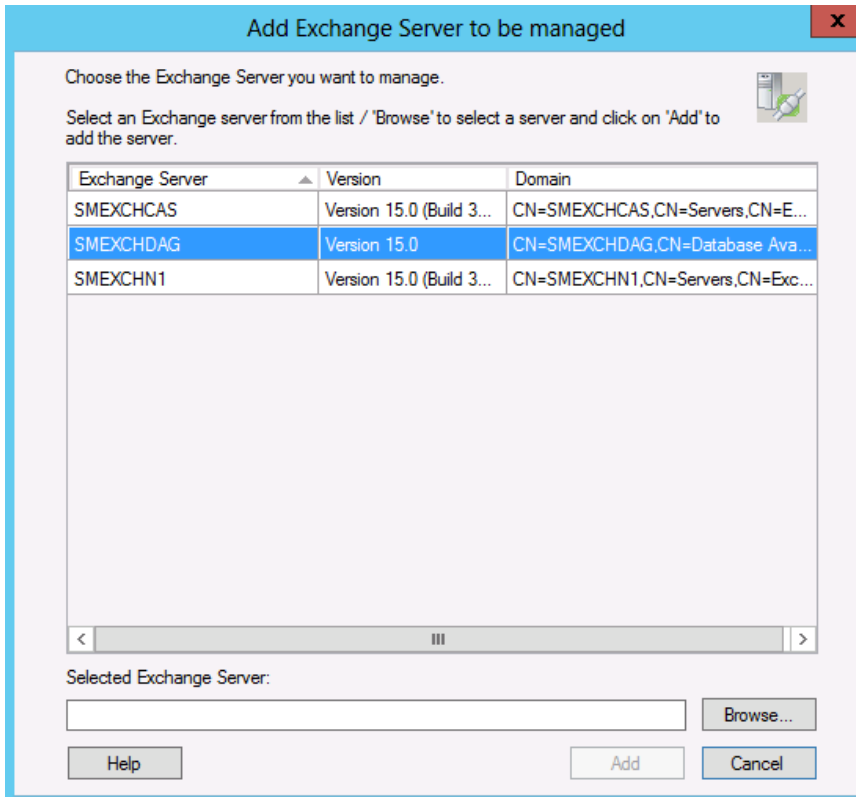
3. If the Exchange server or DAG has not been configured, the SME Configuration wizard starts automatically. On the Welcome page, click Next.

4. On the Database Verification Server page, specify the Microsoft Exchange server to be used to perform Exchange database verification, or select the Select a Verification Server Later Using the Options Menu checkbox.

    Note: Database verification is not a support requirement for databases with at least two copies in a DAG. Microsoft recommends verification of the transaction logs and SnapManager for Exchange performs log verification during the restore operations. By default, when performing a DAG backup with SnapManager for Exchange, verification will be off.

5. On the Select a Storage Group/Database to Move to a LUN page, associate the databases with the correct LUNs according to the SME data configuration plan. Click Next.

    Note: NetApp recommends that all DAG member servers have the same drive letter and mountpoints.

6. On the Select a Set of Logs from One or More Storage Groups/Databases to Move to a LUN page, associate the transaction logs with the correct LUNs according to your SME data configuration plan. Click Next.

    Note: In environments with high LUN counts, transaction logs for multiple mailbox databases can be placed on a single LUN. When deploying LUNs this way, NetApp recommends limiting the number of log streams per LUN to between 5 and 10.

7. On the Configure the SnapInfo Directory to Store the Backup Information page, select the SnapInfo files and the target LUN, and click Next.

    Note: Multiple databases can share the same SnapInfo directory. In most SnapManager environments, the transaction log files are stored on multiple LUNs in multiple volumes. In this configuration, the use of NTFS hard links to archive transaction logs requires a separate

SnapInfo directory for each database. Each SnapInfo directory should be placed on the same NTFS volume as the transaction logs for that database.

8. On the Add Microsoft iSCSI Service Dependency page, select No, Do not make the Exchange System Attendant Dependent on Microsoft iSCSI Service. Click Next.

   Note: This option is not applicable in Exchange server 2013.

9. On the Configure Automatic Event Notification (Recommended) page, configure the Automatic event notification options. Click Next.

10. On the Operations Monitoring and Reporting Settings page, configure the Monitoring and reporting settings. Click Next.

   Note: The monitoring and reporting settings apply only to the Exchange server on the current owner node of the cluster. To set monitoring and reporting on other nodes, connect to the individual node to configure the monitoring and reporting settings.

11. Review the configuration summary on the Completing the Configuration wizard page and click Finish.

12. Click Start Now to migrate the databases, transaction logs, and SnapInfo files to the specified target LUNs.

   Note: If you move the location of Exchange databases in this step, the step may take longer to complete.

13. When the configuration is completed, SME lists the connected Exchange server/Database DAG and is ready to create database backups and perform restores for the server.

Configuring SnapManager for Exchange Backup

After installing SnapManager for Exchange on all nodes of the DAG, follow these steps to configure the backup.

1. In the Scope pane, select the Exchange server node/DAG name you want to back up.

2. Click Backup.

3. SnapManager displays the list of databases in the Backup view in the Result pane and the corresponding actions that you can perform for SnapManager backup in the Actions pane.

   Note: If the SnapManager MMC snap-in is connected to a DAG, you must use the Database Filter to specify the criteria to display the Exchange 2013 databases for backup.

4. Select the databases you want to back up.

5. The Result pane shows whether the database is dataset-enabled, the name of the enabled dataset, the SnapMirror status, the SnapVault status, and other details about the database.

6. Click Backup Wizard in the Actions pane.

7. The Welcome window appears.

8. Follow the instructions in the Backup wizard to initiate a backup process.

9. In the Completing the Backup wizard dialog box, click Finish after you verify that all the settings in the window are what you want.

10. The Backup Status window appears.

11. Click Start Now to start the backup.

12. The backup is performed and the Snapshot copy is written to the volume.

SnapManager Backup completes each task and checks it off on the list shown in the Backup Task List view. You can alternate between the task check-off list and the progress report. If the backup is successful, the Task view shows the check-off list with the tasks completed.

For detailed SnapManager for Exchange configuration steps, refer to Appendix A: "Installation and Configuration Details" in this guide.

Frequent Recovery Point Configuration

Recovery point objectives (RPOs) have become a defining part of a data protection plan for Microsoft Exchange. The ability to have a near-zero RPO is highly desired by Microsoft Exchange administrators because it minimizes the amount of data that is lost between the last full verified backup set and the point of failure. To help achieve desired service-level agreements (SLAs) and RPO times, SME has frequent recovery points (FRPs). These FRPs are optimized backup sets that are created through SME. The backup sets only contain the transaction log files that have been created since the last full backup or the last FRP backup was created. Those transaction log files are copied into the SnapInfo directory, and then a Snapshot copy is created of the LUN containing the directory. Because FRP backup sets contain a smaller amount of information, backups can be created very frequently, as often as every 10 minutes. The higher frequency of FRP backups reduces RPO times.

Backup Planning for Databases in DAGs

By planning the backup strategy for Microsoft Exchange databases, you can minimize the chances of losing data if a restore operation is necessary while still controlling the resources needed to create and maintain the backups. The strategy to choose depends, in part, on the number of DAG nodes, the number of databases, the size of the databases, the network links between the DAG nodes, the service-level agreements, and how quickly the database can be reseeded.

- If DAG resides on nine nodes, you can choose a gapless backup strategy based on the SnapManager for Exchange remote additional copy backup feature. Remote additional copy backup greatly simplifies the administration of backups.
- If the DAG is larger than nine nodes, choose a server-oriented backup strategy; depending on the recovery requirements, add frequent recovery point (FRP) backups to the server-oriented backups to meet tighter RPOs.

Configuring Single Mailbox Recovery for Microsoft Exchange

Table 8 lists the prerequisites for single mailbox recovery.

Table 8) Prerequisites for single mailbox recovery.

| Description of Prerequisites |
| --- |
| Both .NET Framework 3.5 SP 1 and .NET Framework 4.0 must be installed on the Single Mailbox Recovery (SMBR) host server. |
| The SMBR host server must have a Fibre Channel (FC) or iSCSI SAN connection to the NetApp storage system that contains the Exchange backup data. iSCSI is sufficient for performing most of the SMBR recovery tasks. |
| SnapDrive for Windows must be installed on the SMBR host server. |
| Microsoft Exchange system management tools must be installed in order to run SnapManager for Exchange services. |
| The 32-bit version of Microsoft Outlook 2007 or later must be installed on the SMBR host server. |
| At a minimum, a 100Mb/sec TCP/IP LAN network connection is required. |
| SMBR installation requires 200MB of free hard drive space. |

Note: NetApp recommends installing a FlexClone license on the NetApp storage system. The FlexClone feature prevents a busy LUN Snapshot copy condition from occurring while the LUN Snapshot copy is mounted.

To configure Single Mailbox Recovery for Microsoft Exchange, follow these steps.

1. Download the SMBR installation package from the NetApp Support site.
2. Run the installation package.
3. Select the source database and log path, as shown in the following screenshot.

4. Select the target, which can be a PST file or an Exchange server. SnapManager for Exchange presents a Snapshot backup, which Single Mailbox Recovery uses as the source material for restoration. At this point a single item, an entire mailbox, or multiple mailboxes can be fully restored to the production Exchange server.
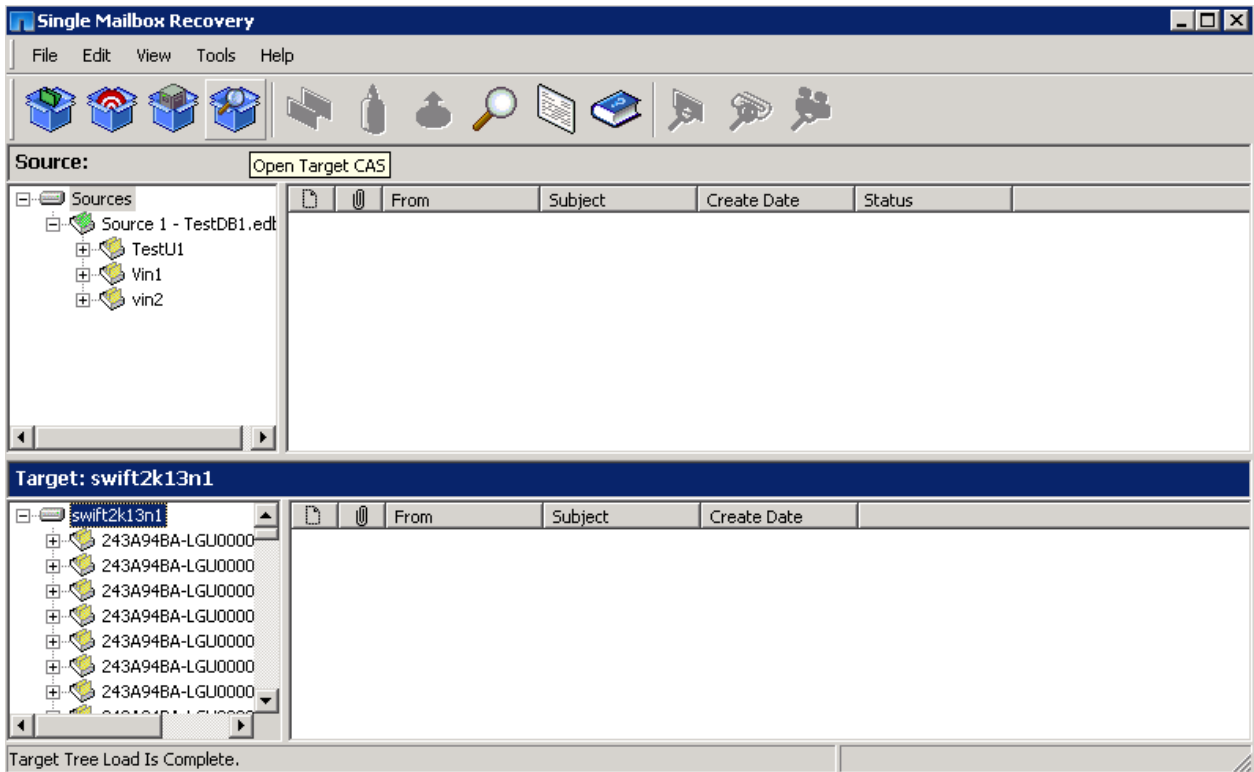
Step 10: Test and Validate the Solution

Pretest of Solution Readiness

After setting up and configuring the designed Microsoft Exchange environment, it is important to test every component for its readiness in terms of functionality, resiliency, and availability.

Table 9 lists tests that can be performed at each level to check the readiness of the architecture to meet its design specifications.

Table 9) Readiness tests performed.

Test Case	Basic	Functionality	High Availability
Name resolution	X		
AD replication	X		
DNS replication	X		
Windows user logon	X		
Mailbox logon and access		X	
DAG creation		X	X
Mailbox database creation		X	X

Test Case	Basic	Functionality	High Availability
Mailbox creation on mailbox servers		X	X
Activate mailbox database copy		X	X
Perform server switchover			X
Send e-mails		X	
Receive e-mails		X	

Storage Connectivity and Validation Tests

Table 10 lists the tests performed so that the basic storage connectivity is tested and validated before the solution is stress tested.

Table 10) Connectivity and validation tests performed.

Test Case	Basic	Functionality	High Availability
SnapDrive Create LUN		X	
SnapDrive Destroy LUN		X	
SnapDrive Expand LUN		X	
SnapDrive LUN Connect		X	
SnapDrive LUN Disconnect		X	
SnapDrive Create Snapshot		X	
SnapDrive Delete Snapshot		X	

Backup and Recovery Tests

Table 11 summarizes the backup and recovery tests validated with the solution.

Table 11) Backup and recovery tests.

Test Case	Basic	Functionality	High Availability
Daily full backups using SnapManager for Exchange Snapshot copies		X	X
Copy backups using SnapManager for Exchange		X	X
Frequent recovery point backup		X	X
Backup verification using SnapManager for Exchange		X	X
Mailbox database restore		X	X
Reseed database using Snapshot copies		X	X

Test Case	Basic	Functionality	High Availability
Retain Snapshot copies and logs as per the retention logic		X	X
Individual mailbox recovery		X	X
Individual e-mail message recovery		X	X

Table 12 lists SnapManager for Exchange backup tests.

Table 12) SnapManager for Exchange backup tests.

Test Case	Details
Task	To test the granularity and scalability of SnapManager for Exchange backup and data retention: • Perform the tasks to create a granular schedule of Exchange Snapshot backups to include standard, daily, and weekly copies with granular and configurable retention of each. • View Exchange notification and logs of these backups. • Monitor the time to do the average backup tasks.
Results	Observe the backup, backup cleanup, and total backup times.

Table 13 lists SnapManager for Exchange restore tests.

Table 13) SnapManager for Exchange restore tests.

Test Case	Details
Task	To test the granularity and scalability of SnapManager for Exchange backup and data retention: • Perform point-in-time restoration of an entire database. • Perform restoration of Exchange databases and play back all log files for up-to-the-minute restoration. • Reseed the passive copy of the database using Snapshot copies to avoid Microsoft Exchange out of the box reseeding. • Monitor time to do the restoration. • Perform single mailbox, single item recovery using the "RUN SMBR" feature and standalone SMBR software.
Results	Observe the point-in-time restore and up-to-the-minute restore.

3   Solution Operation

3.1   Capacity Management

This section describes how to grow and manage the capacity as business needs to grow.

Flexible Volume Management

Flexible volumes can be sized according to capacity requirements. The size of a flexible volume can be increased or decreased. The resize can be accomplished from the command line (telnet, console) or from System Manager.

To resize the volume from the command line, enter the following command:

```
vol size -vserver <vserver name> -volume <vol_name> -new-size [+ | -] <New size>
```

In the preceding command, vol_name is the name of the volume and size is the space to be added to or removed from the volume. Size also includes a modifier to identify whether the space added is in kilobytes (k), megabytes (m), gigabytes (g), or terabytes (t). The plus or minus sign indicates whether space will be added to or subtracted from the volume.

Example: The volume name is SMEvol1 and the size is 250GB. The new desired size is 300GB. The command to change the size of the volume is:

```
vol size -vserver <vserver name> -volume vol_SMEvol1 -new-size +50g
```

Expanding LUNs

To expand the LUNs, complete the following steps.

Under SnapDrive in the left SnapDrive for Windows MMC pane, select the instance of SnapDrive to manage. Then double-click Disks and select the disk to manage.

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand Disks and select the disk you want to manage.
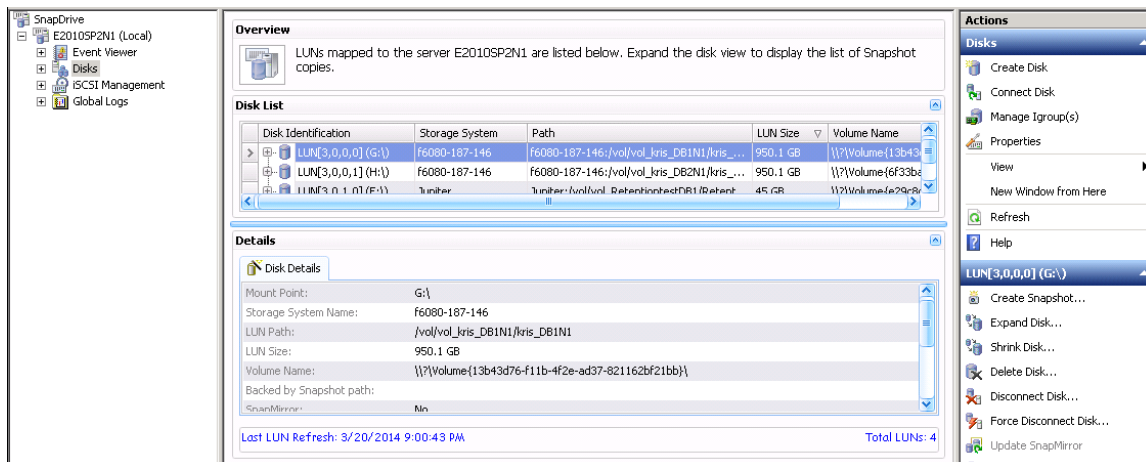
2. From the menu choices at the top of MMC, navigate to Action > Expand Disk.
3. Next to Maximum size in the Resize Disk window, leave Reserve space for at least one Snapshot copy selected.

    Note: When you select this option, the disk size limits displayed are accurate only when they first appear on the Select LUN Properties panel.

4. In the New size box, either type a value or use the slider bar to increase or decrease the amount of space the disk uses.
5. Select Take a Snapshot before resizing the LUN checkbox to take a Snapshot copy before you resize your disk.
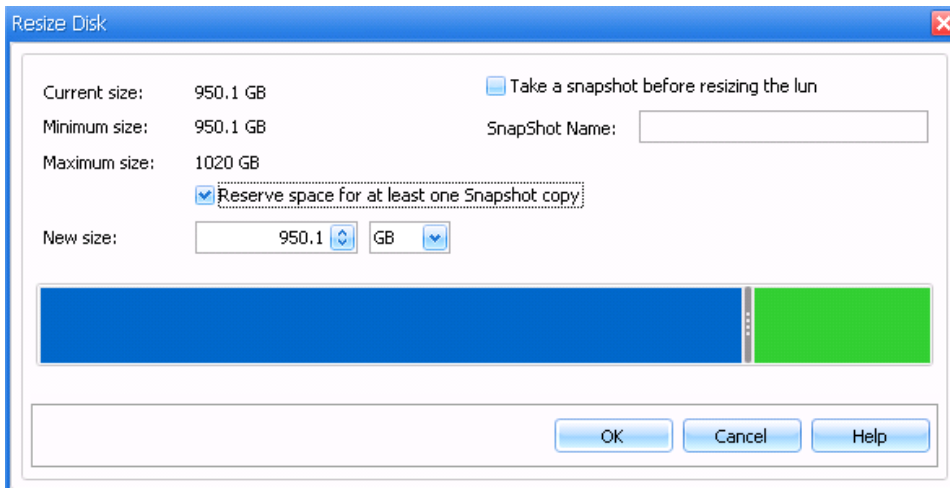
6. Click OK.
7. Create a new Snapshot copy of the resized disk.

If you increase the size of the LUN, you may need to close and reopen the computer management MMC (compmgmt.msc) before the increased LUN size becomes visible in the Disk Management snap-in.

3.2 Backup and Recovery Operations

Configuration Wizard in SnapManager for Exchange

The primary function of the configuration wizard is to migrate Microsoft Exchange databases to Data ONTAP LUNs so that the databases can be backed up and restored by using SnapManager.

Note: Make sure that all databases are migrated to NetApp LUNs from local disk. Microsoft Exchange databases must reside on NetApp LUNs for SnapManager to be able to back them up.

For Initial Configuration

Before using SnapManager to back up and restore any Microsoft Exchange databases, you must use the SnapManager configuration wizard to migrate the databases and transaction logs from local disks of Microsoft Exchange servers to the LUNs that you configured on your storage system with SnapDrive.

To View or Change the Database Configuration

After the initial configuration, you can rerun the configuration wizard at any time to review or make changes to your Microsoft Exchange database configuration.

To Validate the Database Configuration

If you add databases or move databases to different LUNs without using SnapManager, run the configuration wizard so that the databases are stored in valid locations and to create a mapping between those databases and their respective SnapInfo subdirectories.

Use the SnapManager configuration wizard to move Exchange databases, transaction logs, or system files so that these files are placed in locations that meet SnapManager configuration requirements. Incorrectly located Microsoft Exchange databases, transaction logs, or system files impair SnapManager operation.

For detailed SnapManager for Exchange backup configuration steps and recovery steps in a DAG environment, refer to **Appendix C: "Solution Operation Details"** in this guide.

Using the Single Mailbox Recovery Tool

Single Mailbox Recovery works with existing Microsoft Exchange server backup architecture and procedures, allowing you to recover individual mailboxes, folders, messages, attachments, calendars, notes, and tasks directly to your production Exchange server or to any PST file. This eliminates time-consuming and expensive single-mailbox (brick-level) backups, and it also lets you search and create a copy of all archived e-mail that matches a given keyword or criterion. To restore mail items from a Microsoft Exchange database (EDB) file in a SnapManager backup:

1. Connect to the LUN in the Snapshot copy on the NetApp storage system.
2. Use Single Mailbox Recovery to restore the mail items directly from the SnapManager-created Snapshot copy.

   Note: Single Mailbox Recovery can be launched through SnapManager for Exchange using the Run SMBR option in the Action pane to locate and then restore items at any level of granularity directly to an existing mailbox on the Microsoft Exchange server.

The following operations can be done using the SMBR tool:

- Restore messages with copy and paste
- Restore a folder
- Restore a mailbox
- Restore an EDB file
- Restore Public Folder Mailboxes

For detailed instructions on how to use the Single Mailbox Recovery tool, see the Single Mailbox Recovery 7.0 User Guide.

4   Conclusion

E-mail challenges are multiplying, with ever-increasing demands for storage, resiliency, and lower costs. If you need a durable and scalable messaging infrastructure that is easier to manage, reliably available, and cost effective, the NetApp Microsoft Exchange solution is the right answer. With this solution, you can:

- Easily scale storage capacity on the fly and expand with no downtime, at the lowest incremental cost.
- Access and protect your data by using redundant hardware and intelligent software that constantly work to preserve the integrity and availability of your data, with no single point of failure.
- Perform fast and accurate restores of critical e-mail information, bolstered by nondisruptive high-speed backups that are simple to manage.

Appendix A: Installation and Configuration Details

Detailed Steps to Install SnapDrive

Downloading SnapDrive for Windows

Download SnapDrive for Windows from the NetApp software website. Consult your NetApp systems engineer to acquire the license to start using SnapDrive capabilities.

Installing SnapDrive for Windows

Install SnapDrive for Windows on all the Microsoft Exchange Mailbox servers to provision and manage storage LUNs.

Before setup begins, verify the compatibility of all hardware and software involved by using the [NetApp Interoperability Matrix Tool](#).
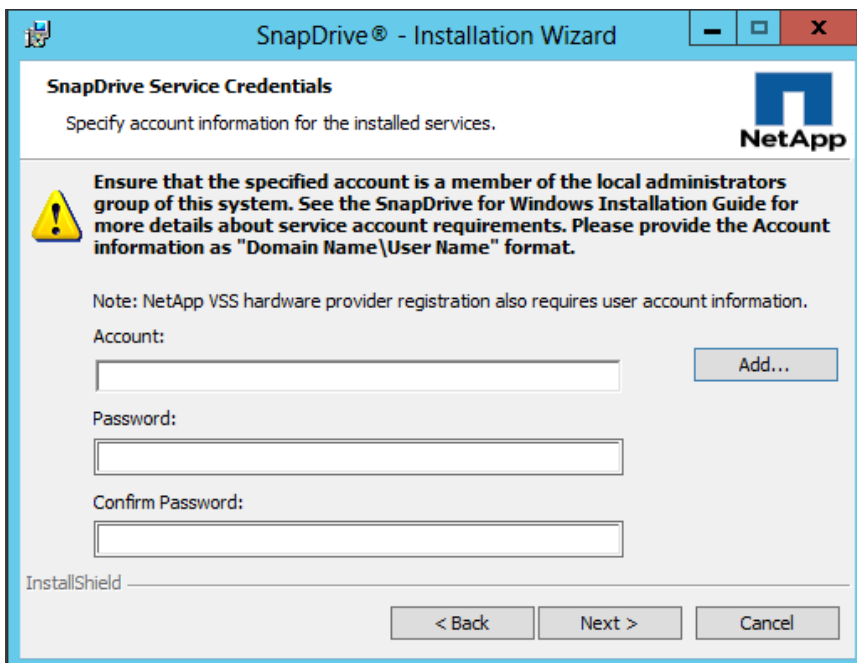
To install SnapDrive for Windows, complete the following steps.

1. Browse to the location of the SnapDrive installation package and double-click the executable file to launch the SnapDrive installation wizard.

2. On the Welcome to the SnapDrive Installation Wizard screen, click Next.

3. Read and accept the license agreement and click Next.

4. On the SnapDrive License page, select the type of licensing to use.

5. Enter the license key. If host-side licensing is used, enter the license key per server. Click Next.

    Note: When storage system licensing is selected, SnapDrive can be installed without entering a license key. SnapDrive operations can be performed only on storage systems that have a SnapDrive or SnapManager license installed.

    Note: With cluster-based systems, the storage system licensing for SnapDrive is bundled with the other SnapManager product licenses. The bundle is a single license called the SnapManager_suite license.

6. On the Customer Information page, enter the user name and organization name. Click Next.

7. On the Destination Folder page, select a host directory in which to install SnapDrive.

    Note: By default, this directory is `C:\Program Files\NetApp\SnapDrive\`.

8. On the SnapDrive Service Credentials page, enter the Account credentials. Alternatively, click Add to select a specific user account from Active Directory. Click Next.

    Note: The specified account must be a member of the local administrators group on this system.

9. On the SnapDrive Web Service Configuration page, keep the default port settings and click Next.
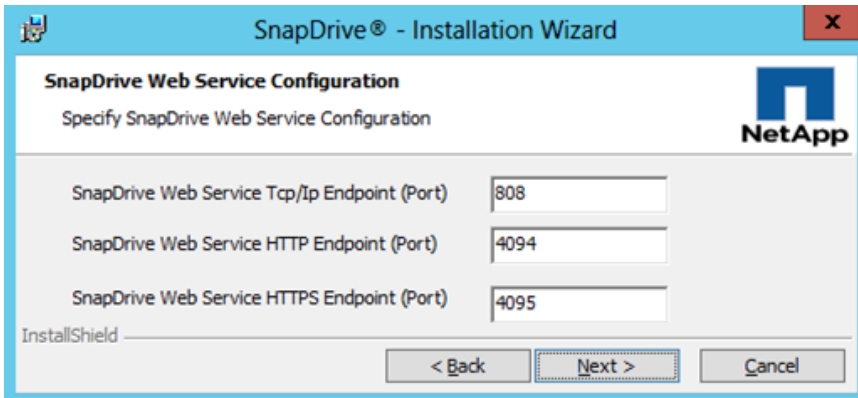
10. On the Preferred Storage System IP Address page, click Next.
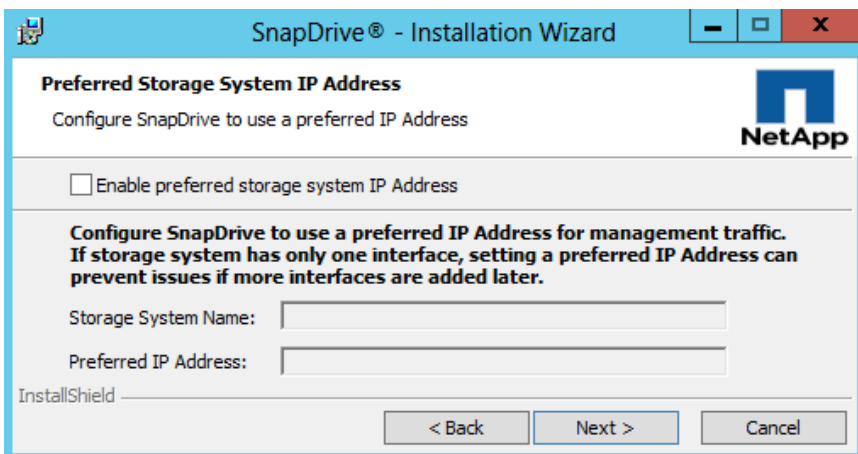
11. On the Transport Protocol Default Setting page, select HTTPS and click Next.

Note: NetApp recommends using HTTPS. The HTTPS protocol allows the use of the Data ONTAP interface for all interactions between the storage system and host, including sending passwords securely.

Note: The RPC protocol is not supported for SnapDrive when clustered Data ONTAP systems are used.
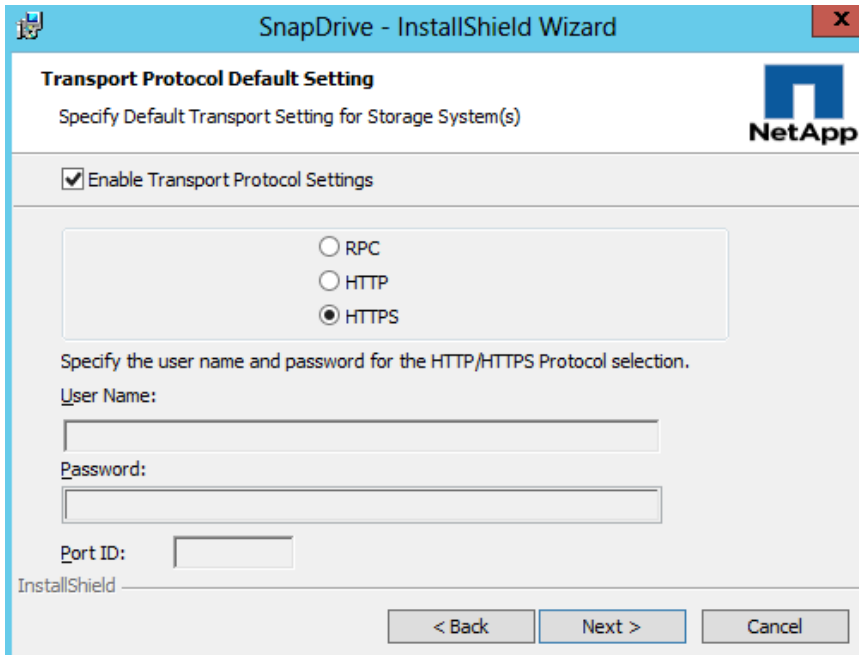
12. On the OnCommand configuration page, clear the Enable Protection Manager Integration checkbox and click Next.

    Note: Protection Manager can be configured after the SnapDrive installation is complete.

13. On the Server Information page, clear the Configuration Option checkbox and verify that all of the fields are unavailable. Click Next.

    Note: VMware integration and pass-through disk setup for Hyper-V can also be configured after the SnapDrive installation is complete. Refer to SnapDrive Documentation for enabling and disabling vCenter or the ESX logon from SnapDrive MMC if using VMware or to enable the Hyper-V server pass-through disk if using a Hyper-V configuration.

If the VMware ESX® guest OS is detected, the Installation Wizard prompts for the IP address and a user name with the appropriate vCenter™ or ESX server privileges. On the VirtualCenter or ESX Server Web Service Credentials screen, type the IP address of the vCenter or ESX server and the user name and password for SnapDrive to authenticate for web service. To use vMotion®, use vCenter.

Note: Selecting Enable VirtualCenter or ESX Server Settings enables SnapDrive to use RDM pass-through LUNs. Select this option to use RDM pass-through disks. By default, this option is not selected.
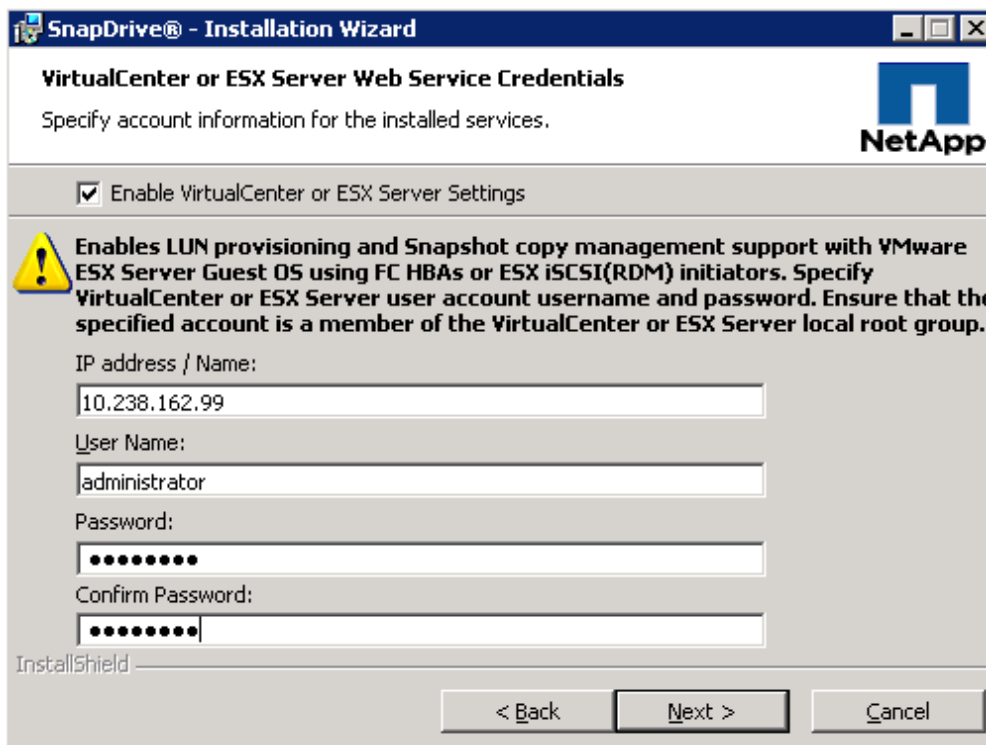
14. If the Hyper-V guest OS is detected, the Installation Wizard prompts for the IP address and a user name with the appropriate Hyper-V server privileges. Type the IP address of the Hyper-V server.
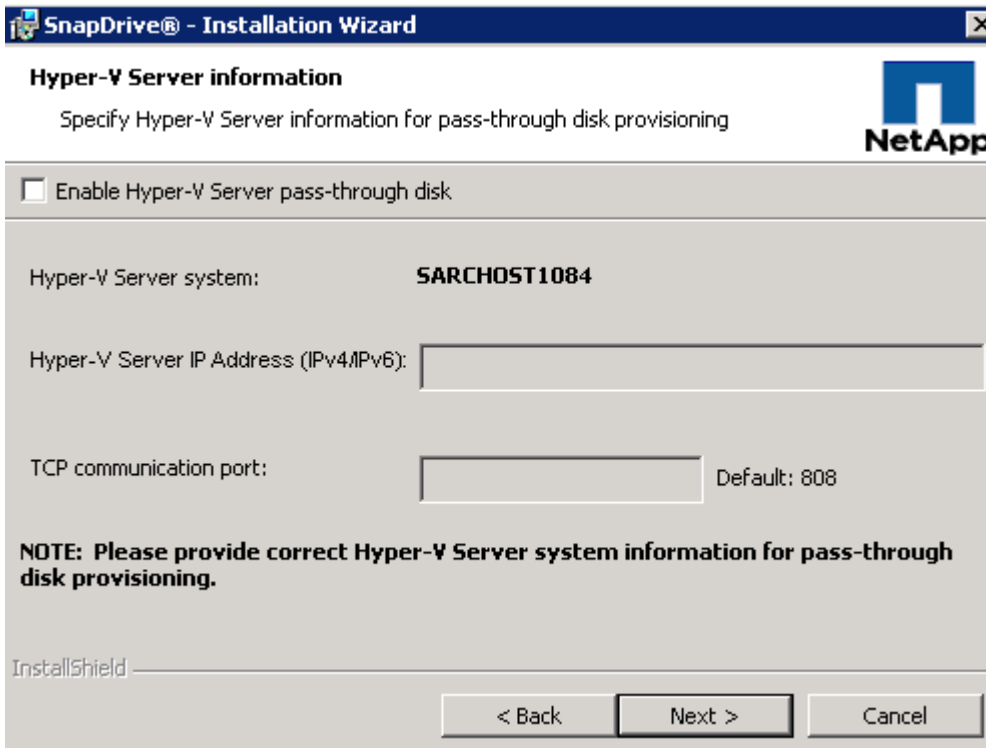
15. On the Ready to Install page, click Install.

16. When the SnapDrive Installation Completed page is displayed, click Finish.

Set Transport Protocol Settings in SDW

To configure Transport Protocol Settings in SDW, complete the following steps.

1. Log in to the host system and launch SnapDrive.
2. From the SnapDrive console, right-click the host name and select Transport Protocol Settings.
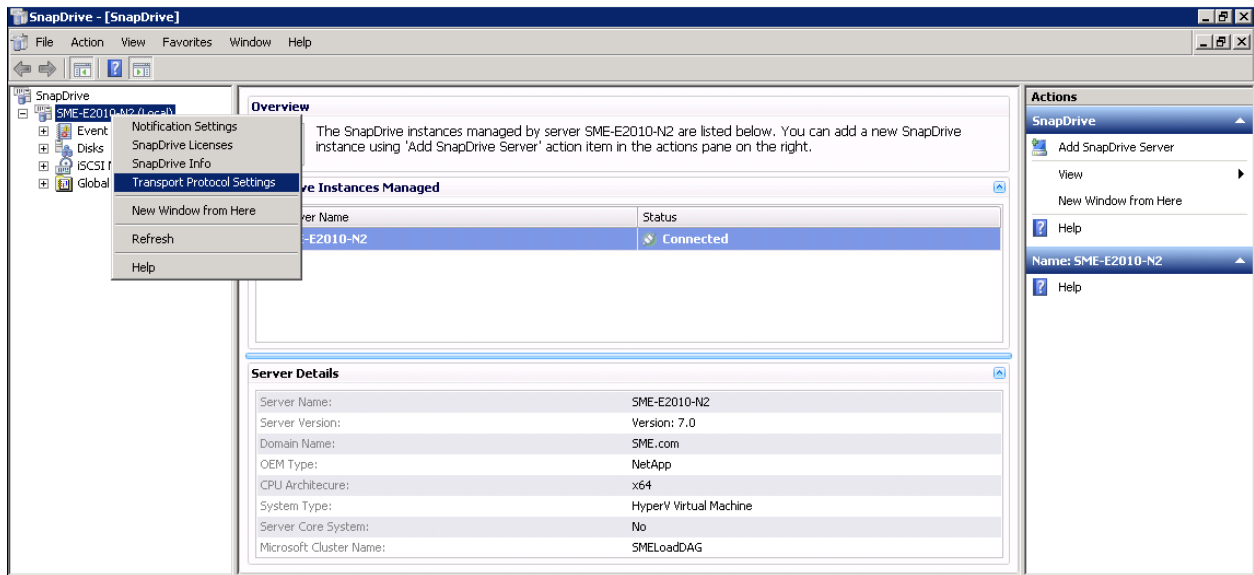
3. From the Storage Systems tab, click Add.
4. In the Add Storage System dialog box, add the IP address of the SVM Management LIF, and then click OK.
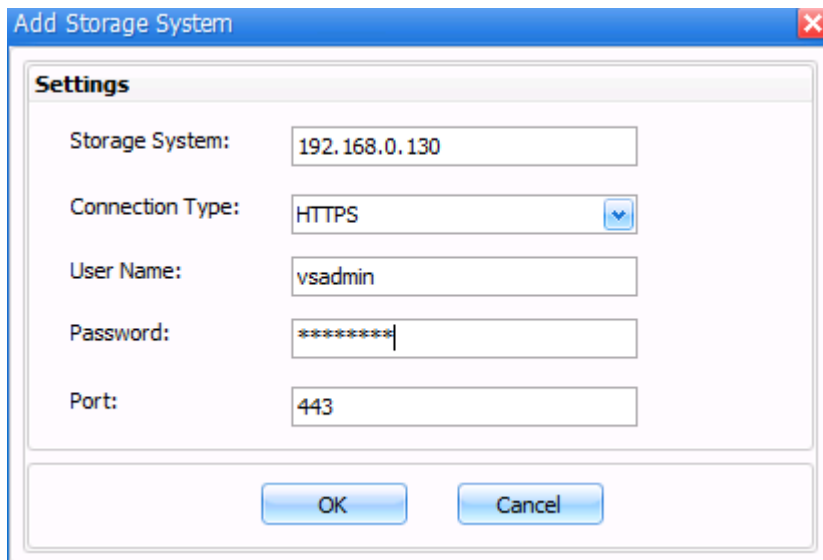
5. Verify that the SVM has been successfully added to the SnapDrive host.

Transport Protocol Settings

Storage Systems | Default

Configure storage systems to be connected using HTTP or HTTPS or RPC

Storage System	Type	Port	User Name
192.168.0.130	HTTPS	443	vsadmin

Add   Edit   Delete

OK   Cancel   Apply
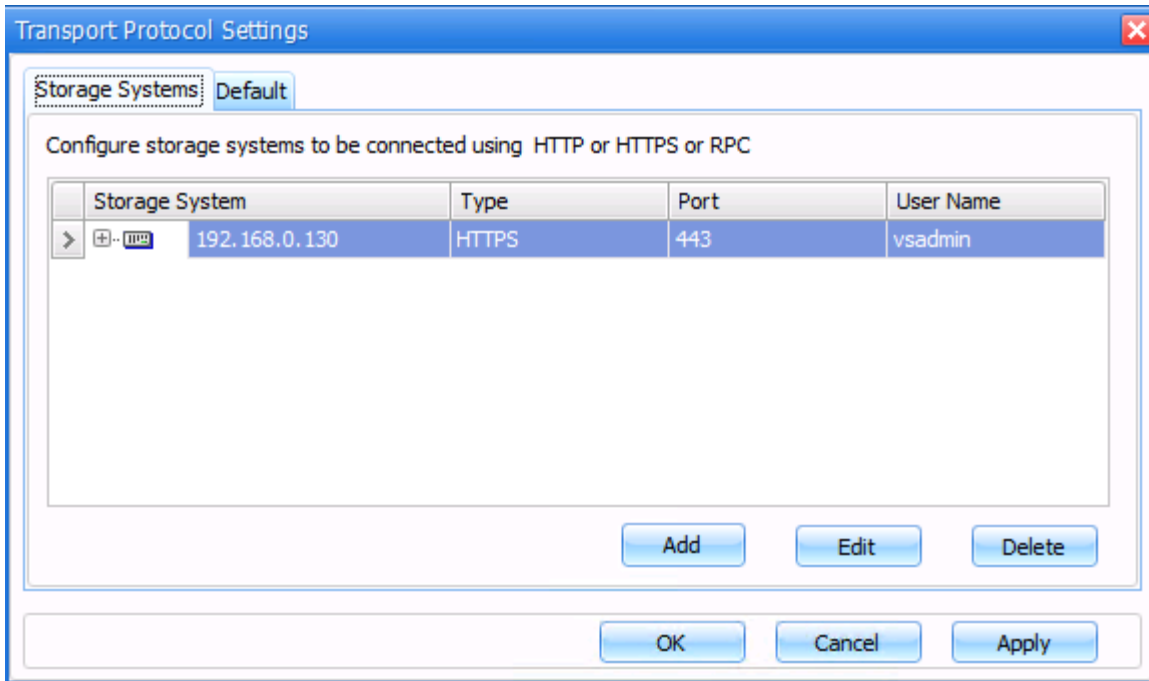
Accessing and Managing SnapDrive for Windows

SnapDrive for Windows can be managed from the Microsoft Windows Computer Management MMC console.

1. From the Start menu, select Control Panel > Administrative Tools > Computer Management. Otherwise, select Start > Run, enter `compmgmt.msc`, and click OK.

2. In the left panel, under Storage, select SnapDrive to list the SnapDrive options.

Creating LUNs

Before starting to provision LUNs by using SnapDrive, make sure that the FCP or iSCSI service is started on the storage system.

Note: You may need to license the FCP or iSCSI protocol based on your requirements. Consult your NetApp systems engineer or your NetApp software subscription package for license details.

Two types of LUNs can be provisioned to the host by using SnapDrive for Windows:

*   Dedicated
*   Shared

Dedicated LUNs are dedicated to the server to which they are connected or mapped and are used in all Microsoft Exchange DAG deployments. Shared LUNs are used with MSCS. SnapDrive for Windows is cluster-aware and allows all the cluster nodes to connect to a single LUN when a shared LUN is provisioned.

1. Open the Computer Management Console.

2. Expand SnapDrive and expand the server name.

3. Right-click Disks and select Create Disk.

4. Enter the storage system name or IP address in the Create Disk Wizard. If you already added the storage system in the storage systems management window, you can select the storage system from the drop-down list.

5. Select the volume where this LUN will be hosted. Enter a LUN name in the LUN Name field and enter a meaningful description for the LUN. Click Next.

6. Select Dedicated in the LUN type panel and click Next.

7. In the Select LUN Properties window, select a drive letter or mountpoint.

8. Select Limit or Do Not Limit for the option Do you want the maximum disk size to accommodate at least one Snapshot copy. In this case, we selected Do Not Limit to make the best use of thin provisioning. Enter the size of the disk to be created and click Next.

9. In the Select Initiators window, select the initiators. If you need to achieve multipathing, select all the initiators. The selected initiators must be of the same protocol. (A selection cannot have one FC initiator and one iSCSI initiator.) Click Next.

10. In the Select Initiator Group Management window, select Automatic and then click Next.

11. Click Finish to create the SnapDrive-provisioned LUN.

12. From the SnapDrive GUI, you can locate the drive that you just created.

Detailed Steps to Install Microsoft Exchange 2013 Server

Preparing the Active Directory Domain

It is necessary to prepare the Active Directory domain to accommodate the Exchange server. Active Directory preparation can be run separately from the command line or the installer can do it automatically. Refer to the Microsoft TechNet link to prepare the Active Directory domain.

Installing the Mailbox and Client Access Server Roles

After making sure that the servers meet the prerequisites for Microsoft Exchange server 2013 installation, perform the steps outlined in Microsoft TechNet http://technet.microsoft.com/en-us/library/bb124778(v=exchg.150).aspx.

After installation is complete, Postinstallation Tasks are necessary to license the server, configure mail flow and client access, and verify the installation.

Creating Microsoft Exchange Server 2013 Data Availability Group

1. To create a DAG, use the shell to specify a name and either DHCP or specific static IP addresses.

Example:

```
New-DatabaseAvailabilityGroup -Name SMEDAG1 -WitnessServer SMECAS1 -WitnessDirectory
C:\DAGWitness\SMEDAG1.domain.com
-DatabaseAvailabilityGroupIPAddresses 10.225.187.52
```

2. After the DAG is created, add mailbox servers to it with the Exchange Management Shell.

Example:

```
Add-DatabaseAvailabilityGroupServer -Identity SMEDAG1 -MailboxServer SMEEX1
Add-DatabaseAvailabilityGroupServer -Identity SMEDAG1 -MailboxServer SMEEX2
```

After sizing the storage for capacity and performance, make sure that the path to each database and transaction log LUN is identical on each mailbox server that will host a copy of that particular database.

Detailed Steps to Install SnapManager for Exchange (SME)

Installing and Configuring SME

You can install SnapManager by using the software installation utility in the interactive mode. The InstallShield wizard guides you through the installation.

Installing SME by Using Interactive Mode

To install SME by using the interactive mode, complete the following steps.

1. Download the SME executable file from the [NetApp Support](#) site.
2. Browse to the SnapManager installation package and double-click the installation package .exe file.
3. In the License Agreement window, accept the license agreement.
4. In the Customer Information window, specify the user name, the organization name, and the SnapManager license type.
5. Optional: If desired, in the Destination Folder page, change the default download directory by clicking Change and entering the new location.
6. Take note of the full path of the folder in which SnapManager will be installed.
7. In the SnapManager Server Identity window, specify the user account you want to use to run SnapManager.
8. Type and confirm the password.
9. Click Install.
10. Wait until the InstallShield Wizard Completed window appears; then click Finish to exit the software installation utility.
11. Repeat all of the steps on all the DAG nodes.

Configure Backup Settings for SME

The default backup settings for SME must be modified to reflect the time-based Snapshot copy names as opposed to the most recent Snapshot copy names.

To change the default behavior of the backup settings, complete the following steps.

1. Open SME and select Options > Backup Settings.
2. In the Backup Settings dialog box, make sure that only the Use Unique (Timestamp) Naming Convention option is selected.

Configure Notification Settings for SME

SME is configured to send notifications about failures through an e-mail to a recipient or group. SME can also trigger the AutoSupport™ tool (a Data ONTAP feature) from the storage controller in case errors or other events occur, thereby giving NetApp Support all of the necessary storage configuration information.

To configure notification settings for SME, complete the following steps.

1. Open SME and select Options > Notification Settings.
2. Make the necessary changes to the notification settings and click OK.
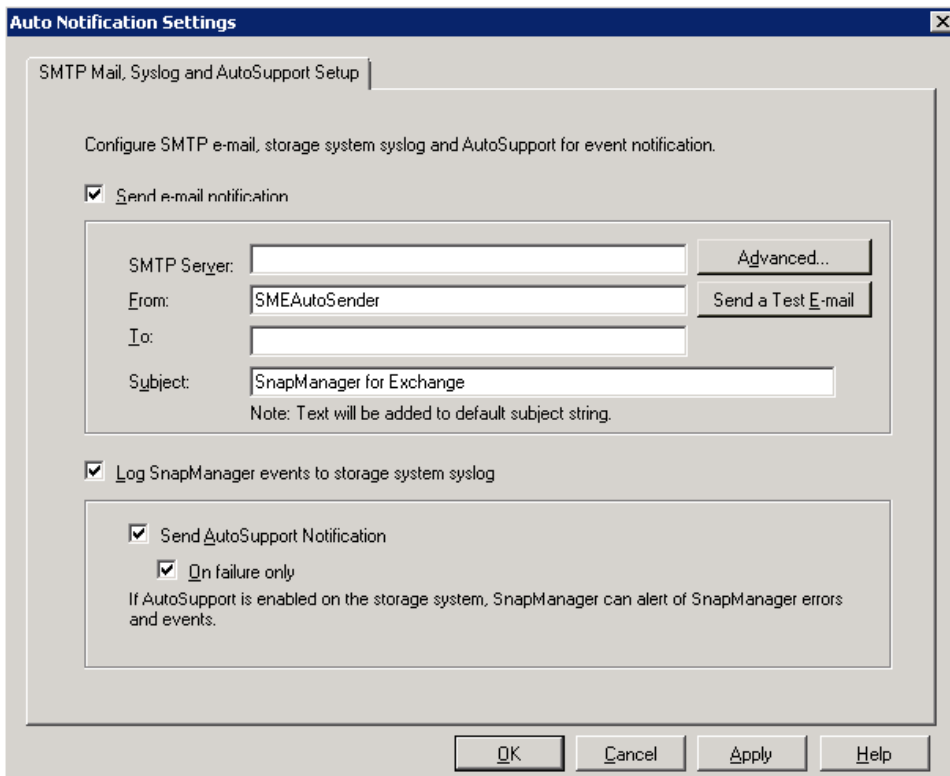
Install and Configure SMBR

To install and configure SMBR, complete the following steps.

1. Download the SMBR installation package from the NetApp Support site.
2. Run the installation package.
3. On the Welcome page, click Next.

   Note: If you are installing SMBR on a dedicated server, install 32-bit Microsoft Outlook 2007 or later.

   Note: Configure Outlook at least once so that it has access to a Microsoft Exchange Server mailbox and so a MAPI profile connection is created. For Microsoft Exchange server 2013, Microsoft Outlook 2007 or later is required.

4. Read the license agreement and click Yes to accept the terms.
5. Select the features you want to install and click Next.
6. Click Finish.

Note: If you plan to install SMAS in your environment, the required license.ini file for the administrative services feature can be purchased and downloaded from the NetApp Support site.

Install Single Mailbox Recovery Administrative Server

The SMAS application is used to centralize the management of role-based access control and SMBR audit-logging operations. If neither of these features will be used as part of SMBR operations, SMAS is not required.

Note: NetApp recommends configuring the system so that the SMAS application resides on a dedicated server that is connected to the NetApp storage system with Fibre Channel (FC) or iSCSI SAN.

SMAS can also be installed in a virtual machine (VM) environment as long as the FC or iSCSI SAN connectivity requirement is met.

To install SMAS, complete the following steps.

1. Download the SMAS installation package from the [NetApp Support](#) site.
2. Start the installation package on the dedicated server. Click Next at the Welcome page.
3. Read the license agreement and click Yes to accept the terms and continue.
4. Select the destination folder and click Next.
5. Specify the user account that will be used to run the SMAS application and click Next.
6. Select the Launch Single Mailbox Recovery Management Console option and click Finish.

Appendix B: Test and Validation Details

Basic Tests to Validate the Solution

This section outlines the test procedures for the basic tests that should be performed to validate the deployment. The following tables are examples of a checklist that a customer can refer to for validating the deployment.

Windows User Logon

Test Case	Details
Task	To test whether users are able to log on to the Windows domain: • Create a Windows user and log on to the Windows domain using the created account.

Mailbox Logon and Access

Test Case	Details
Task	To test whether an Exchange mailbox user is able to access his or her Exchange mailbox account: • Create a user with Exchange mailbox. • Log on using the created user account. • Access Exchange mailbox with Outlook and Outlook web app.

Name Resolution

Test Case	Details
Task	To test the name resolution system: • Use `nslookup` to look up the name of the servers and systems in the Active Directory domain.

Active Directory Replication

Test Case	Details
Task	To test whether Active Directory replication is working: • Run `dcdiag` on all the domain controllers.

DNS Replication

Test Case	Details
Task	To test whether DNS replication is working as deployed: • Run `dcdiag` on all DNS servers.

DAG Creation

Test Case	Details
Task	To test DAG creation and query status information: • Run `Get-DatabaseAvailabilityGroup | fl` to verify the information regarding DAG. • Run `Get-mailboxdatabasecopystatus | fl` to view status information about mailbox database copies.

Verify Replication and Replay Status in Database Availability Group

Test Case	Details
Task	To test the replication status of DAG: • Run `Test-replicationhealth | fl` to verify the replication information regarding DAG.

Verify Incoming and Outgoing Mail Flow

Test Case	Details
Task	To test incoming and outgoing mail flow: • Send sample messages from Internet mailboxes to various internal test mailboxes and between internal mailboxes and verify that the e-mails were successfully received and delivered.

Verify That the Mailbox Databases Were Created and Mounted

Test Case	Details
Task	To test whether mailbox databases were created and mounted: • Run the cmdlet `Get-mailboxdatabase | fl` to verify the status of the mailbox databases.

Appendix C: Solution Operation Details

Configuring Exchange Backups by Using SnapManager for Exchange in DAG Environments

To back up the Microsoft Exchange server databases, complete the following steps.

1. Log in to Designated node as the user Domain\SMEuser and start SnapManager for Exchange.

2. In the left pane, expand the Exchange server or DAG and click Backup. In the center pane, select the entire DAG, or expand the DAG and select individual databases to back up.
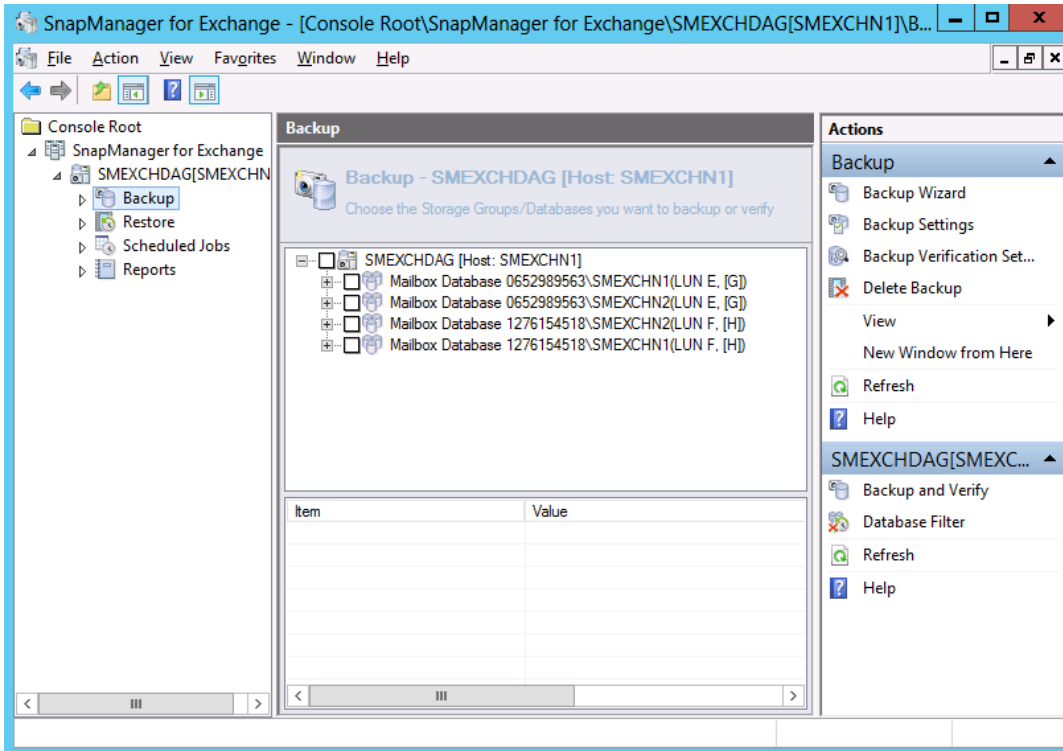
3. To filter the DAG view so that only the relevant databases are visible, right-click the DAG name and select Database Filter.
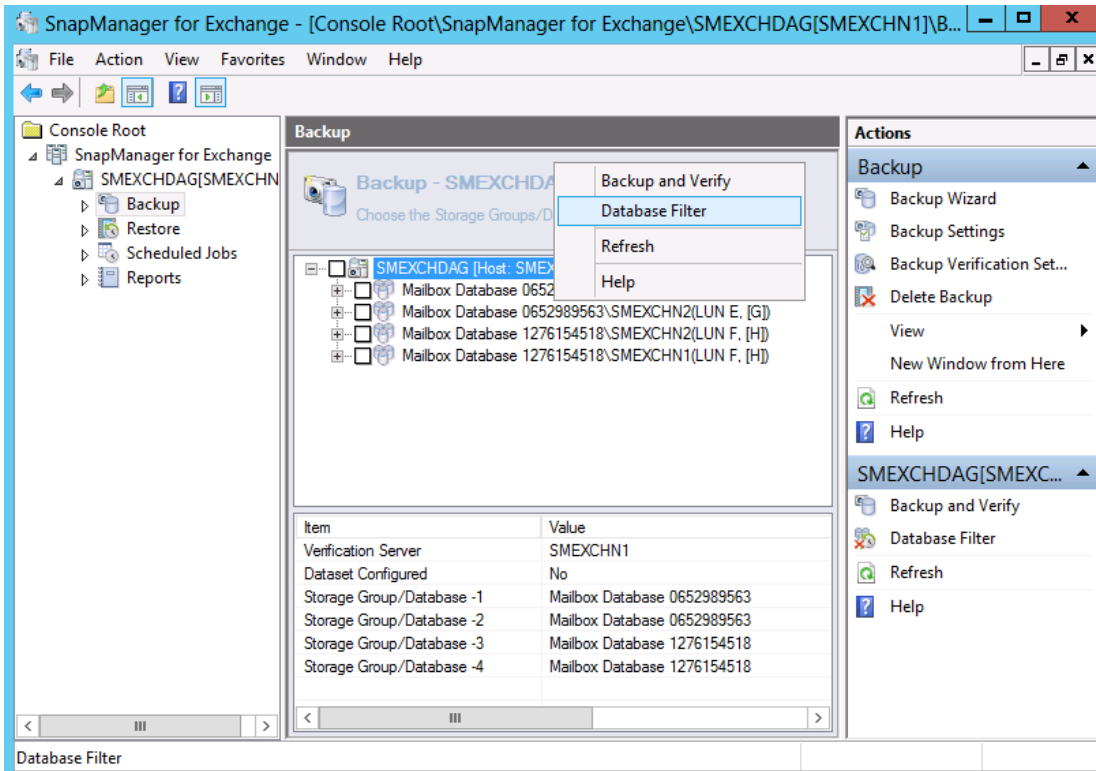
4. Make the desired selections from the drop-down menus and click OK. In this example, the DAG is filtered to display the passive databases in the Microsoft Exchange server.
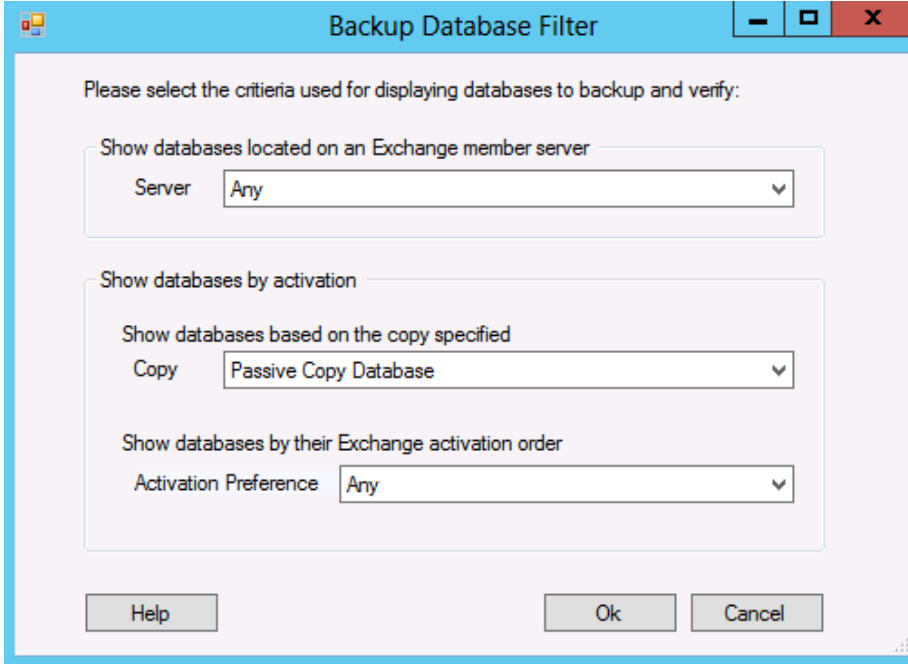
5. Right-click in the Backup pane and select Backup and Verify.

    Note: If a database has an invalid status, SnapManager does not allow the backup operation to continue for that specific database.
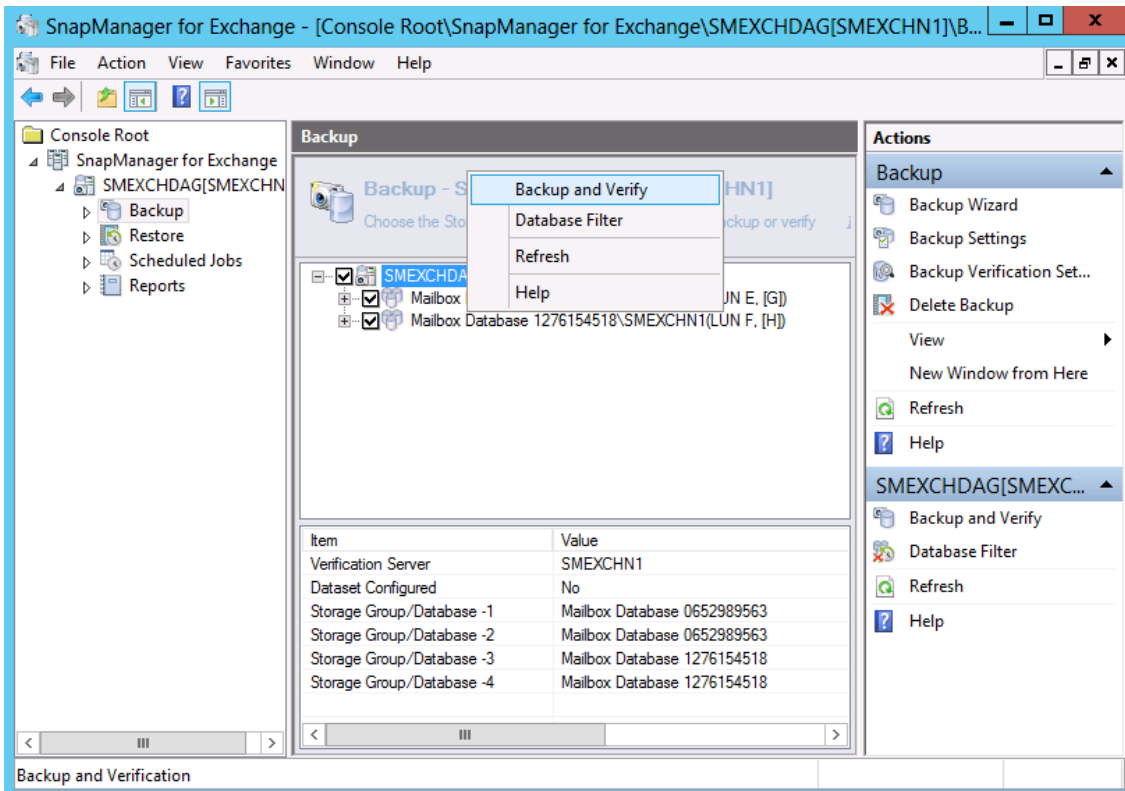
6. Click Advanced Options.
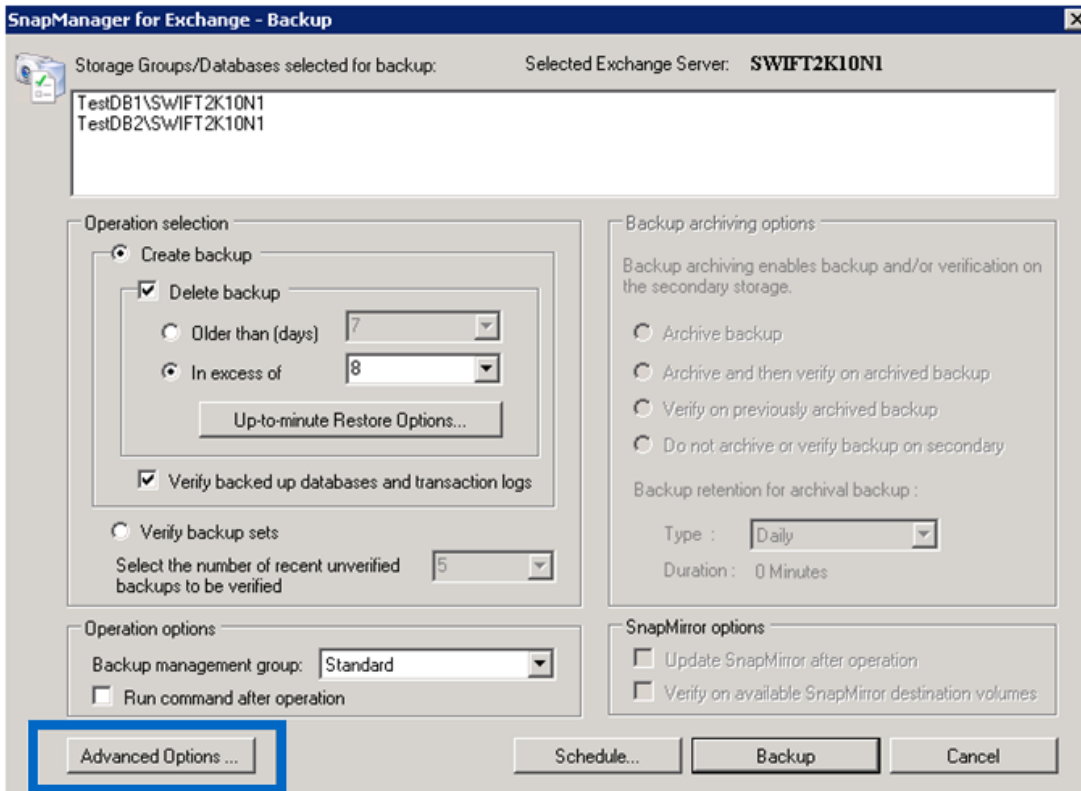
7. Click the Additional Remote Copy Backup tab and configure options to perform up-to-the-minute restore operations.

   a. Select the Create Additional Backup (Copy Based) Backups on the Remote CCR/DAG Member Servers checkbox.

   b. Define the retention policy for backups on the passive nodes.

   c. Click OK.

   Note: In earlier versions of SnapManager, remote backup was created by the Standard Management group. In SnapManager 7.0, remote backup inherits the same management group that was selected for local backups in the Backup wizard.
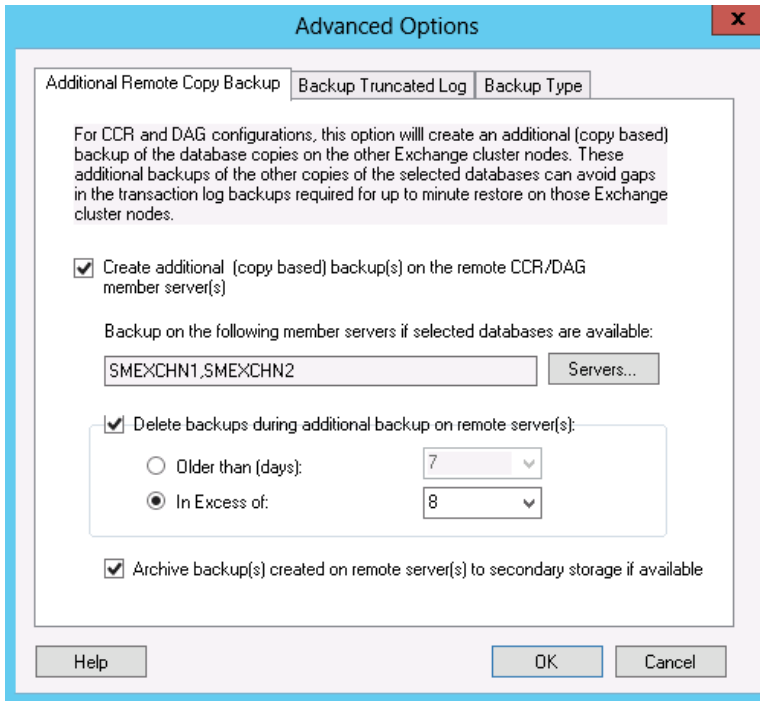
8. Configure the backup settings:

   a. Select Create Backup.

   b. Select the Delete Backup checkbox and define the backup retention policy.

   c. Select a backup management group.

   d. Click Up-to-Minute Restore Options to view or change the backup transaction log settings, if applicable.
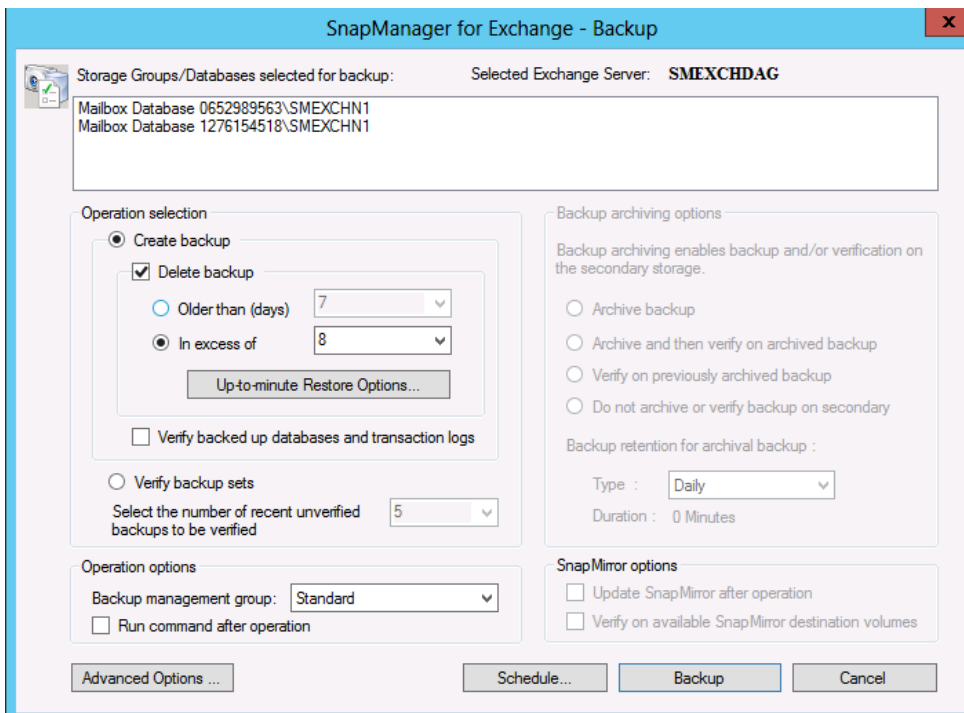
9. Click Schedule to use Windows Task Manager to schedule the backup process.

10. Click Yes in the confirmation message to open the Schedule Jobs window.

> **Note:** SME automatically detects the DAG member servers if the backup selection is for DAG level and offers to create a backup schedule for each of them.
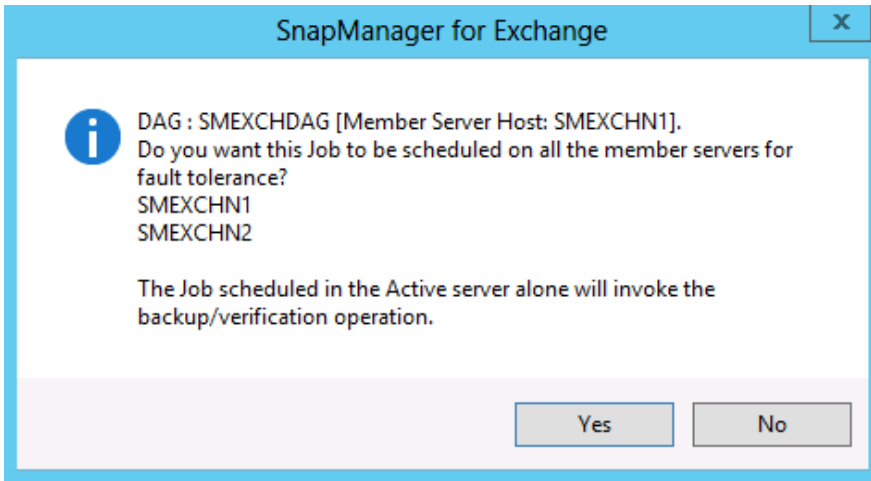
11. On the Schedule page, enter the name of the backup job, enter the user ID and password for the job, and click OK.

> **Note:** If this job name already exists as a Windows scheduled task and you want to replace it with a new job, select the Replace Job If It Exists checkbox and click OK. Navigate to Control Panel > Administrative Tools > Task Scheduler to modify the schedule or to cancel the scheduled job. The backup job schedule can be viewed in the Scheduled Jobs view in SME.
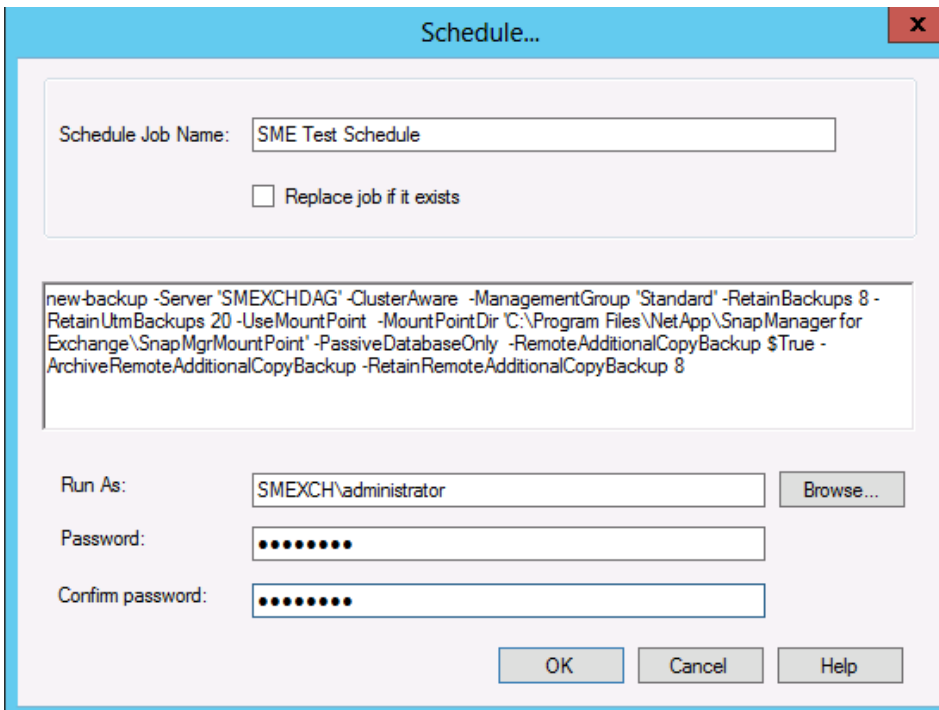
12. To specify backup schedule parameters, select Scheduled Jobs from the left pane in SME. Click the Schedule tab to specify the following, and then click OK.

    a. When the job will run

    b. If the job will repeat

    c. At what frequency the job will repeat

13. Click Backup to perform an immediate backup of the Microsoft Exchange server databases.
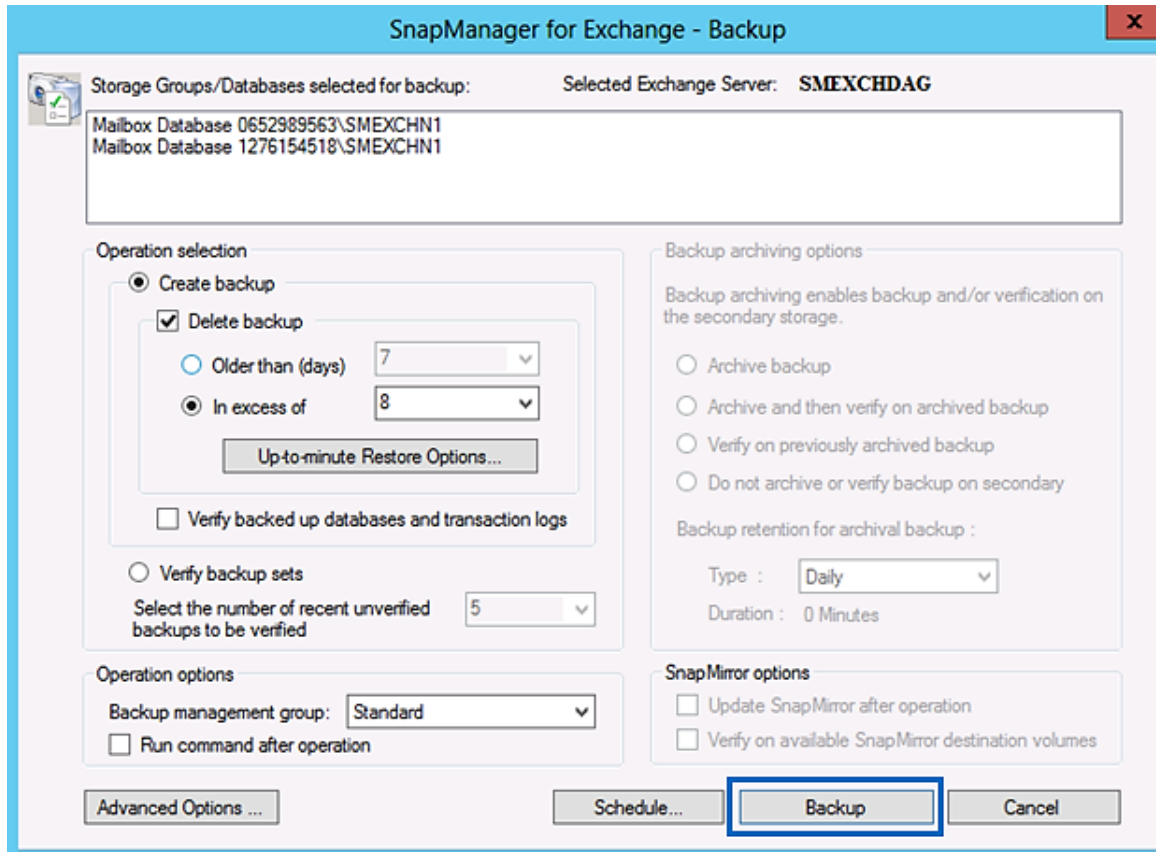
14. On the Backup Status page, click Start Now to back up the selected databases. The backup operation finishes and the Snapshot copy is written to the volume. SnapManager Backup completes each task and checks it off in the Backup Task List.

    Note: You can alternate between the Backup Task List and the Backup Report tabs. If the backup process is successful, the Backup Task List tab shows the completed tasks. If notifications are enabled, an e-mail message is sent, and the event is posted to the Windows Application Event log.
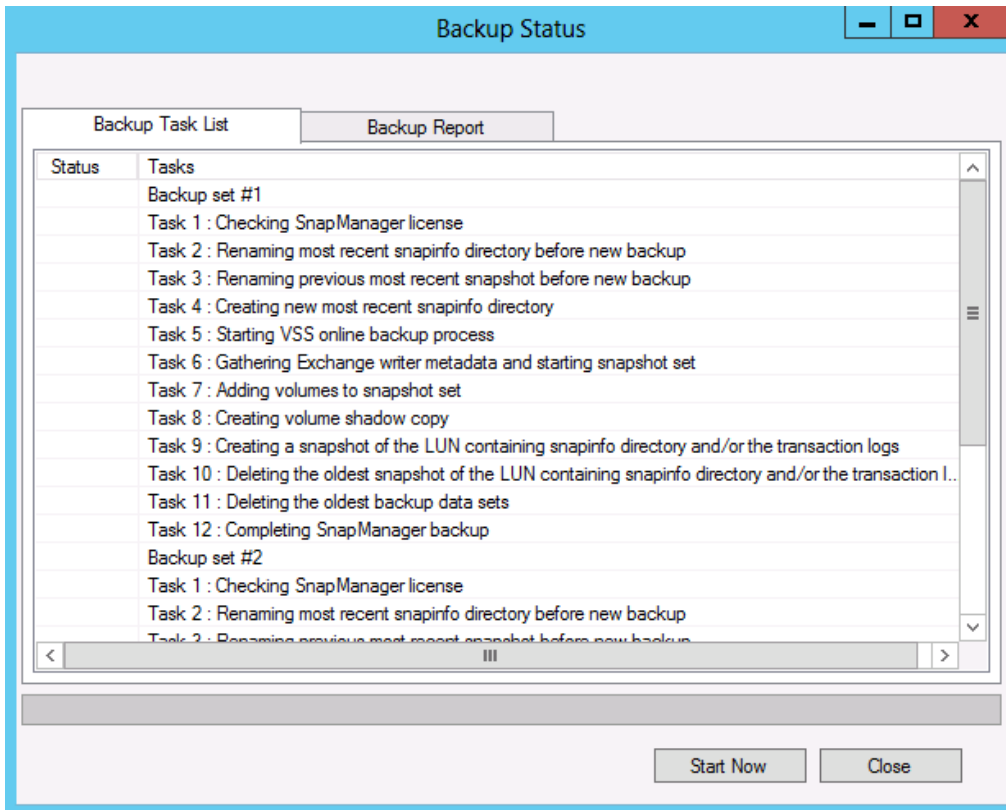
Restore from SnapManager Backup Copy in DAG Environments

You can access SnapManager Restore in order to restore databases from a backup copy in two ways:

• SnapManager Restore wizard

• Restore window accessed from the Actions pane

Do not perform a restore operation while a backup operation is in progress. If you cancel a current backup operation in progress, SnapManager pauses all active scheduled backup jobs on the Exchange server, or on all nodes in the DAG environment, and cancels the current backup copy before performing the restore operation. When the restore operation is complete, SnapManager reenables the paused scheduled backup jobs. All the other inactive jobs remain unchanged.

If you want to restore after the current backup operation completes, SnapManager pauses all active scheduled backup jobs on the current Exchange server (on all nodes in the DAG environment), but waits for the completion of the current backup operation before performing the restore operation. When the restore operation is complete, SnapManager reenables the paused scheduled backup jobs. All other inactive jobs remain unchanged.

Note: Close all windows on the Exchange server running SME. Disable any SME operations that are scheduled to run against the Exchange data that you want to restore, including any jobs scheduled on remote management or remote verification servers.

To restore from a SnapManager backup copy, complete the following steps.

1. Start SME.

2. In the left pane, select the Exchange server or DAG and click Restore.

Note: SME displays the Exchange server databases. When SME connects to the DAG, all backups in the DAG are displayed. When it connects to a member server of the DAG, only the backups on that server are displayed.

3. Double-click the backup copy under the database that you want to restore and select Restore.
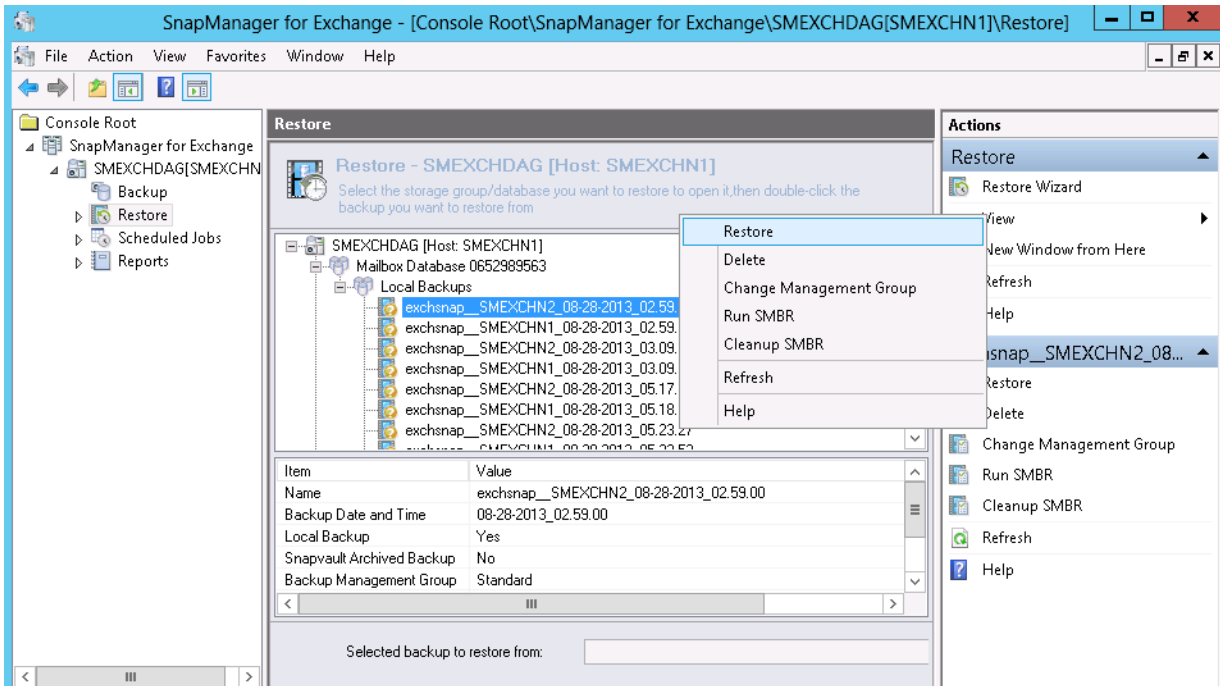
4. Select the databases that you want to restore and select either Up-to-the-minute restore or Point-in-time restore.
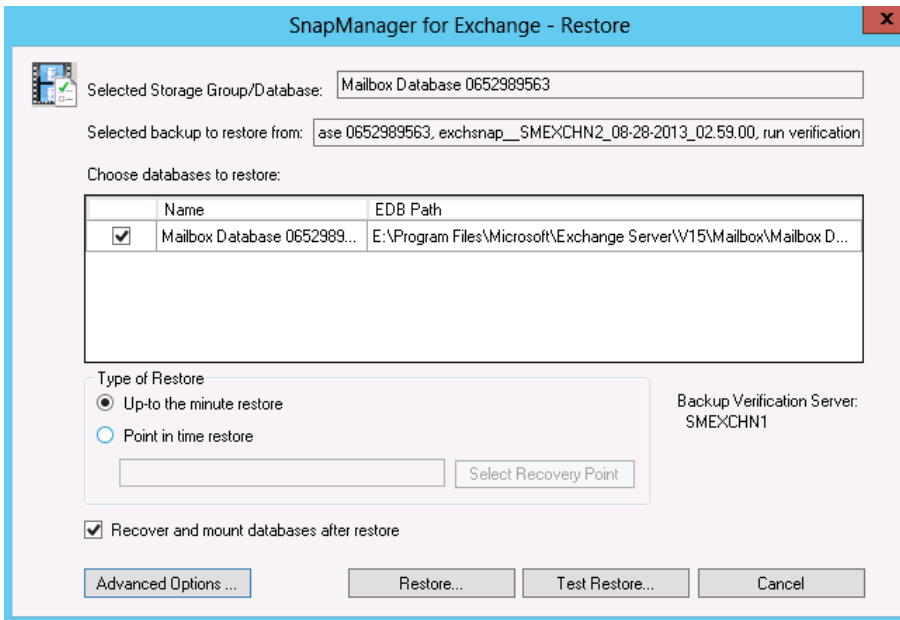
5. If you do not want to perform exhaustive verification of the transaction log sequence and database metadata before the restore process, click Advanced Options. Under Operation Options, clear the

Verify Transaction Log Sequence and Database Metadata Before Restore and Exhaustive Verification checkboxes and click OK.
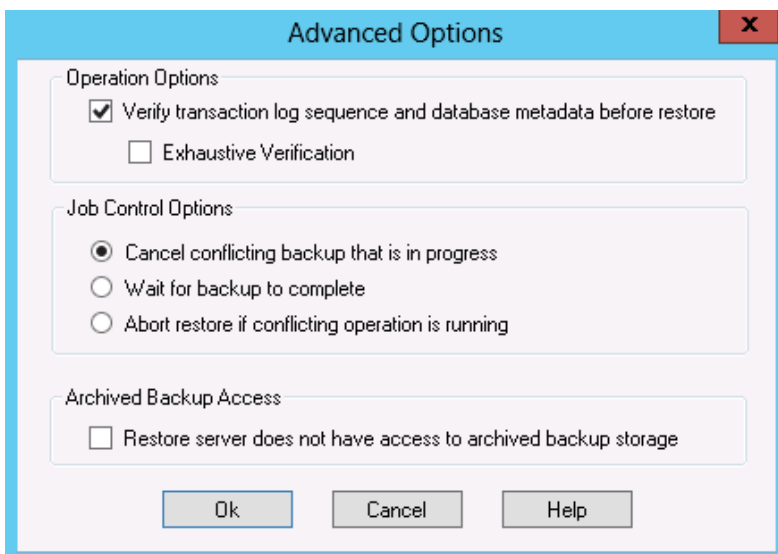
6. If the backup copy is unverified, SME prompts to verify it before the restore operation begins. Click Yes in the confirmation message.

   Note: Database verification is not a support requirement for databases with at least two copies in a DAG.
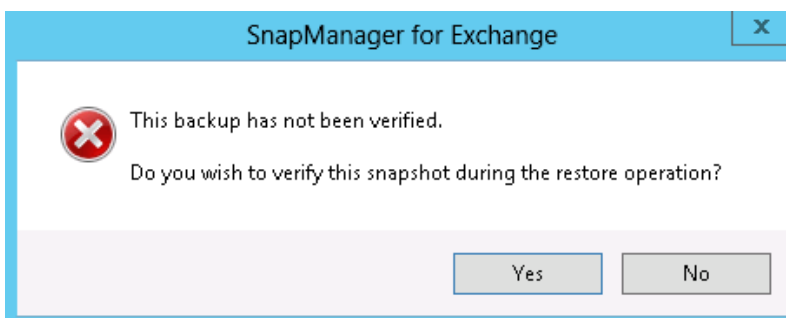
7. SME validates whether the database to be restored is the active or passive copy of the database. If the Recover and Mount Databases After Restore option is selected and the passive copy of the database is selected for restoring, a message is displayed so that the administrator is aware of potential data loss. Click either OK or Cancel.
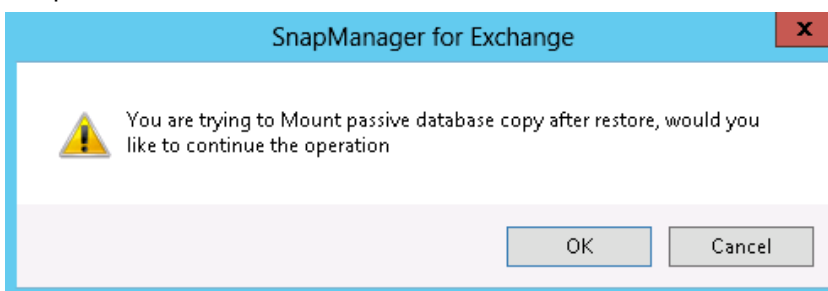
Note: Restoring a passive copy of the database is equivalent to the action of the database reseed functionality in Microsoft Exchange server when the Recover and Mount Databases After Restore option is not selected, provided the backup schedules are planned accordingly to retain transaction log files. Therefore, there is no need to use the Microsoft Exchange server's out-of-the-box replication mechanism (which can be time consuming based on the database size).

8. (Optional) If you are performing a test restore operation, click Test Restore.

   a. From the Select Test Restore Options window, select Check Current Logs (for Up-to-the-minute restore operations only) and run database verification.

   b. To verify databases and transaction logs on available destination volumes, select Run Verification on Computer.

9. The Restore Status page is displayed, showing the tasks that are performed as part of the restore process. Click Start.
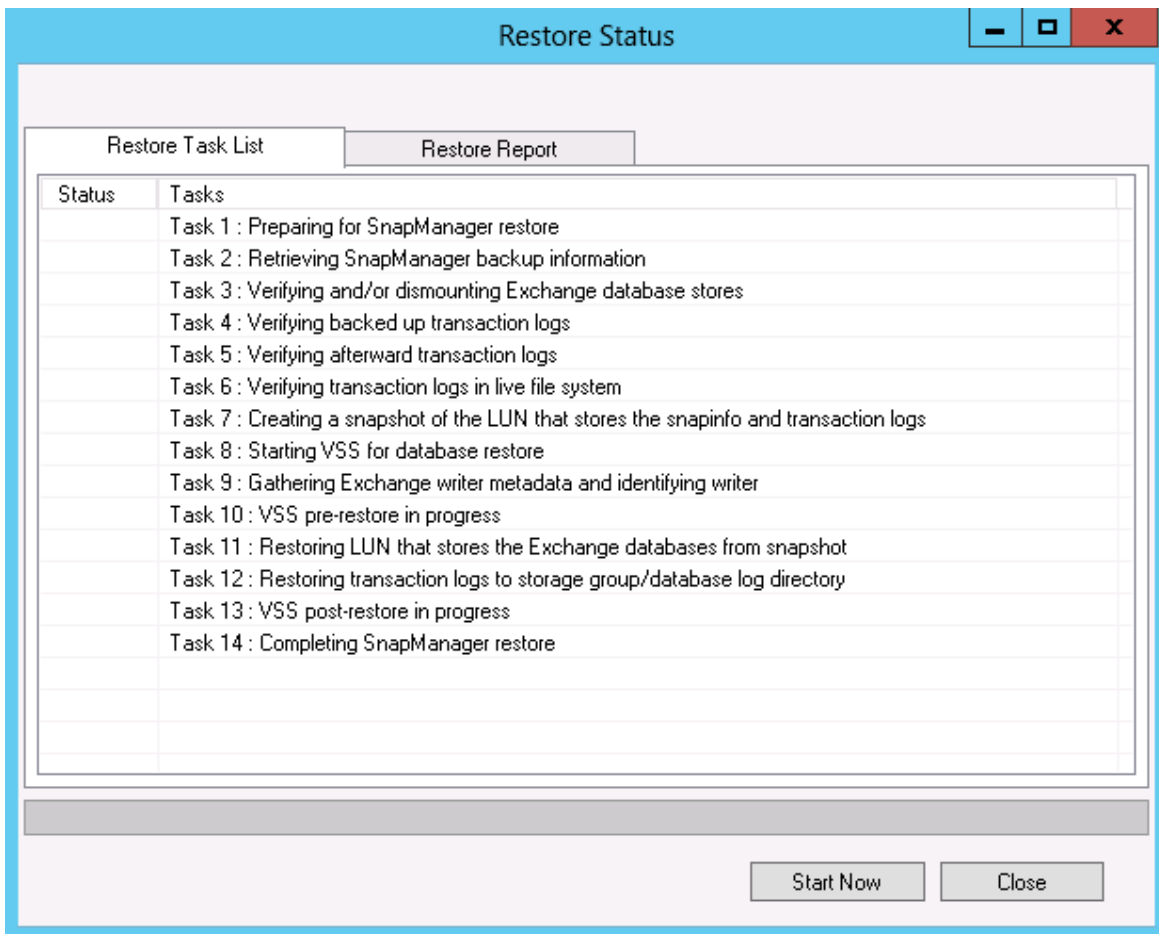
References

The following references were used in this TR.

- Microsoft Exchange Server 2013 and SnapManager for Exchange
  http://www.netapp.com/us/media/tr-4221.pdf

- Microsoft Exchange 2013 System Requirements
  http://technet.microsoft.com/en-us/library/aa996719(v=exchg.150).aspx

- Storage Management Guide
  http://support.netapp.com/documentation/docweb/index.html?productID=61651

- Volume Shadow Copy Service Overview
  http://msdn.microsoft.com/en-us/library/aa384649(v=VS.85).aspx

- Microsoft Exchange 2013 Storage Configurations Options
  http://technet.microsoft.com/en-us/library/ee832792(v=exchg.150).aspx

- Microsoft Exchange 2013 Mailbox Server Role Requirements Calculator
  http://gallery.technet.microsoft.com/office/Exchange-2013-Server-Role-f8a61780

- Data ONTAP Documentation
  http://now.netapp.com/NOW/knowledge/docs/docs.cgi

- Microsoft Exchange 2013 High Availability and Site Resiliency
  http://technet.microsoft.com/en-us/library/dd638137(v=exchg.150).aspx

Version History

Version	Date	Document Version History
Version 1.0	April 2014	Initial release

Go further, faster®

NetApp®

www.netapp.com