



Technical Report

Best Practices Guide for Microsoft Exchange Server Using NetApp SnapCenter

Cheryl George, NetApp
August 2018 | TR-4681

Abstract

This best practices guide is intended for storage and application administrators so that they can successfully deploy Microsoft Exchange Server 2013 and 2016 on NetApp® storage using NetApp SnapCenter® technology for data protection.

TABLE OF CONTENTS

1	Executive Summary	4
1.1	Purpose and Scope	4
1.2	Audience	4
1.3	Prerequisites	4
2	SnapCenter: The NetApp Data Protection Solution for Microsoft Exchange Server	4
2.1	SnapCenter Components	5
2.2	Role-Based Access Control in SnapCenter	10
2.3	SnapCenter Plug-In for Microsoft Exchange Server Architecture	10
2.4	SnapCenter Plug-In for Microsoft Exchange Server Installation and Upgrade Considerations	11
2.5	SnapCenter Plug-In Uninstall Considerations	12
3	Storage Layout Planning	13
3.1	Aggregate	13
3.2	Volumes	13
3.3	LUNs	14
3.4	Capacity Planning	15
3.5	Data Protection.....	15
4	NetApp Storage Efficiency	25
5	Performance.....	25
5.1	SATA Performance Considerations	26
6	Virtualization.....	26
7	High Availability.....	26
8	Disaster Recovery	26
9	Summary	27
	Where to Find Additional Information	27

LIST OF TABLES

Table 1)	Restore options.....	22
Table 2)	Reseed options.....	23

LIST OF FIGURES

Figure 1)	SnapCenter architecture.....	5
Figure 2)	SnapCenter components.....	6

Figure 3) SnapCenter Plug-Ins Package for Windows.	8
Figure 4) Register VMware vSphere in SnapCenter.....	9
Figure 5) SnapCenter data protection of a Microsoft Exchange database availability group.	11
Figure 6) SnapCenter hypervisor settings.	12
Figure 7) Log and full backup retention settings.	20
Figure 8) SnapCenter restore options.....	22
Figure 9) Single Mailbox Recovery architecture.	24

1 Executive Summary

Microsoft Exchange Server is a widely used messaging platform for email communication, group scheduling, and calendaring for collaboration purposes. Failure at any level of storage, server, or networking could result in unacceptable operational and financial losses. Therefore, you should carefully plan data protection, disaster recovery, and high availability to enable quick recovery with little or no data loss. This guide delivers best practice guidance for using NetApp® SnapCenter® technology. SnapCenter tightly integrates with Microsoft Exchange Server to enable application-consistent, online, Volume Shadow Copy Service (VSS)-based backups and point-in-time or up-to-the-minute restores of Exchange databases.

1.1 Purpose and Scope

The best practices and recommendations described in this guide enable database architects and storage administrators to plan a highly available and easy-to-manage Microsoft Exchange Server environment and meet stringent SLAs.

1.2 Audience

This document describes best practices and offers insight into design considerations for deploying Microsoft Exchange Server on NetApp storage systems running NetApp ONTAP® software. The goal of this guide is the effective and efficient deployment of storage and end-to-end data protection and retention planning. The scope of this guide is limited to technical design guidelines based on the design principles and NetApp recommendations for storage infrastructure in Microsoft Exchange Server deployments. End-to-end implementation is out of the scope of this report. This guide assumes that you understand Exchange storage architecture and administration and the data protection concepts of backup and restore. This guide also assumes that you have a working knowledge of the following topics:

- NetApp ONTAP software
- NetApp SnapDrive® for Windows
- NetApp SnapManager® for Microsoft Exchange Server
- NetApp SnapCenter

To determine configuration compatibility across the NetApp stack, see the [NetApp Interoperability Matrix Tool \(IMT\)](#).

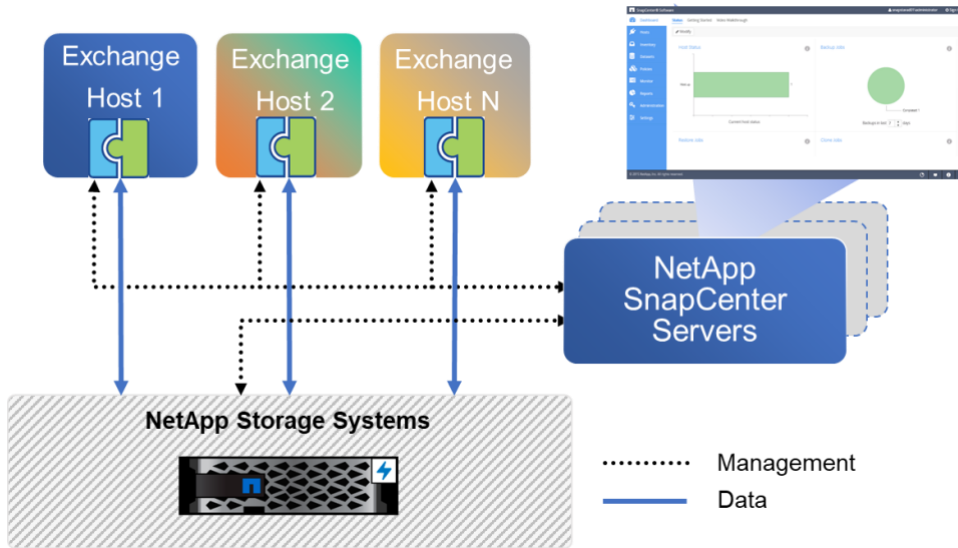
1.3 Prerequisites

The best practices for NetApp SnapCenter data protection presented in this document focus exclusively on Microsoft Exchange Server 2013 and 2016 on Microsoft Windows Server 2008 R2 SP1 and later, with Exchange data stored on the latest NetApp storage operating system, ONTAP 9.x.

2 SnapCenter: The NetApp Data Protection Solution for Microsoft Exchange Server

NetApp SnapCenter is a scalable storage platform that provides centralized control and oversight, while allowing users to manage application-specific backup and restore operations. SnapCenter also provides operational simplicity and lowers TCO by using policy-based management that enables backup automation at scale.

Figure 1) SnapCenter architecture.



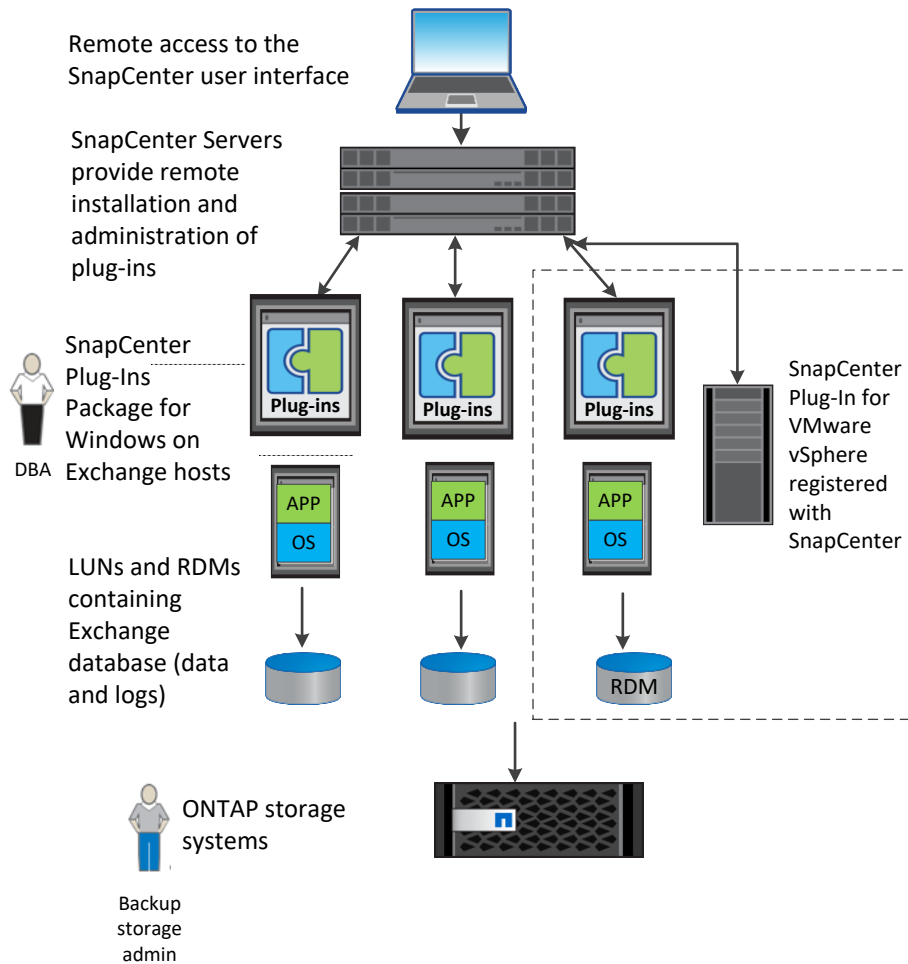
With SnapCenter, you can meet your data-protection SLAs by taking advantage of NetApp ONTAP data management capabilities, including the following technologies:

- **NetApp Snapshot™ technology.** Creates frequent application-consistent, space-efficient backups in minutes without affecting Microsoft Exchange. SnapCenter tightly integrates with the Microsoft Windows VSS framework for the creation of application-consistent Snapshot copies of Exchange databases, with no downtime for the production database.
- **NetApp SnapRestore® technology.** Enables rapid granular restores and application-consistent, point-in-time recovery. Therefore, it is not necessary to keep a lagged copy of the database availability group (DAG) database, saving additional storage.

2.1 SnapCenter Components

SnapCenter consists of the SnapCenter Server and the SnapCenter Plug-Ins Package for Windows as follows:

Figure 2) SnapCenter components.



SnapCenter Server

The SnapCenter Server includes a web server, a centralized HTML5-based UI, PowerShell cmdlets, APIs, and the SnapCenter repository. SnapCenter enables load balancing, high availability, and horizontal scaling across multiple SnapCenter servers within a single UI. You can accomplish high availability by using network load balancing and application request routing with SnapCenter. For larger environments with thousands of hosts, adding multiple SnapCenter servers can help with load balancing.

The SnapCenter platform is based on a multitiered architecture that includes a centralized management server (the SnapCenter Server) and a SnapCenter host agent (SMCore) that runs on the SnapCenter Server. HTTPS and the SnapCenter Plug-Ins Package for Windows are installed on the Exchange hosts to permit communication between the SnapCenter Server and the Exchange hosts.

SnapCenter enables centralized application resource management and easy data protection job execution through policy management, including scheduling and retention settings. SnapCenter provides unified reporting with the use of a dashboard, multiple reporting options, job monitoring, and log and event viewers. Information about SnapCenter operations is stored in the SnapCenter repository.

SnapCenter provides the following key capabilities:

- A scalable platform across various Exchange environments, both virtual and nonvirtual
- Role-based access control (RBAC)—supported security and centralized role delegation to improve productivity

- Application-consistent Snapshot copy management and restore
- Centralized scheduling and policy management for backup and restore operations
- Centralized reporting, monitoring, and dashboard views

Keep the following prerequisites in mind regarding the SnapCenter Server:

- Although the SnapCenter Server can function with a minimum of 8GB of RAM, NetApp recommends using 32GB of RAM.
- Make sure that the Windows OS on the host system on which SnapCenter Server is installed is up-to-date with no pending system restarts.
- The SnapCenter Server host should be part of a domain and not a domain controller.
- Make sure that the SnapCenter Server is installed on a server that is part of a Windows domain. Also, a two-way trust relationship must exist between the SnapCenter Server domain and the domain that hosts the protected Exchange servers. The supported trusts are domain trusts, multidomain forests, and cross-domain trusts.

Note: SnapCenter currently does not support data protection for IPless DAGs in cross domains.

- Log in to the SnapCenter GUI with user credentials in the format of domain\user.
- Each storage virtual machine (SVM, previously called Vserver) supported by SnapCenter must have a unique name because SnapCenter does not support multiple SVMs with the same name on different clusters.
- Verify that a SnapManager Suite license or a SnapCenter Standard license is installed on the ONTAP storage system.
- Do not change the domain in which the SnapCenter Server is installed. Otherwise, the uninstall operation for SnapCenter Server fails.
- Do not rename the Exchange hosts protected by SnapCenter.
- Before you can perform data protection operations using SnapCenter, you must set up the following configurations:
 - Add a connection to the SVM in Storage Systems > Settings. This step gives the SnapCenter Server and the SnapCenter plug-ins access to ONTAP storage. This step also requires the configuration of the NetApp AutoSupport® and event management system (EMS) features.

Note: Make sure that host plug-in installation is not in progress when adding a storage system connection. The host cache might not be updated, and databases might produce the warnings “Not Available for Backup” or “Not on NetApp Storage” in SnapCenter.

- To install the SnapCenter Plug-Ins Package for Windows, use Run As credentials with the Active Directory account that is a domain administrator. You can also use a domain user account that has local administrative privileges on the remote Exchange hosts. For an Exchange DAG, this domain user must have administrative privileges on all the nodes in the cluster. Run As credentials allow you to perform tasks such as adding hosts, installing plug-in packages, and scheduling data protection jobs. For virtualized environments, the Run As credentials should be a domain administrator or a domain user with local administrator privileges on the VMware vSphere server as well.

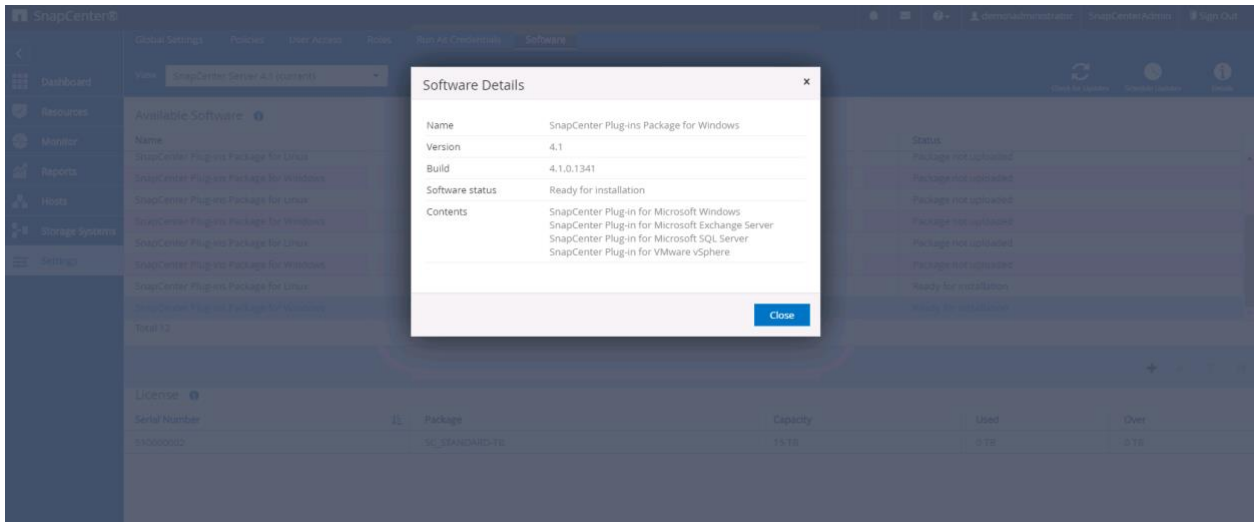
Best Practices

- To simplify the installation process, use the SnapCenter installation worksheet to document necessary details.
- Add the SnapCenter URL to the trusted sites in Internet Explorer (IE), or disable IE enhanced security.
- For security reasons, do not allow your browser to save your SnapCenter password.
- Make sure that you have DNS configured to correctly resolve the SVM name to the SVM management LIF IP address.
- Make sure that you log out of SnapCenter either by clicking Sign Out or by shutting down the web browser to end your connection with SnapCenter.

SnapCenter Plug-Ins Package for Windows

Use the SnapCenter Add Host wizard to install the SnapCenter Plug-Ins Package for Windows on the remote stand-alone Exchange host or all the nodes in the DAG. You must be assigned to a role that has plug-in install and uninstall permissions, such as the SnapCenter administrator.

Figure 3) SnapCenter Plug-Ins Package for Windows.



SnapCenter Plug-In for Microsoft Exchange Server

The NetApp SnapCenter Plug-in for Microsoft Exchange Server (SCE) is a host-side component of the NetApp storage solution that offers application-aware online backup management for Microsoft Exchange Server databases. With the plug-in installed on your Exchange Server host, SnapCenter automates Microsoft Exchange Server database backup and restore operations. Note the following key features of the plug-in:

- Application-consistent backup of Exchange databases and transaction logs hosted on NetApp LUNs
- Support for the full and log, full, and log and copy backup types
- Retention of full and log backup copies
- Updates to NetApp SnapVault® and NetApp SnapMirror® relationships to provide a fast, centralized, and cost-effective disk-to-disk backup by replicating Snapshot copies to the secondary storage system
- Up-to-the-minute and point-in-time restore of Exchange databases that use transaction logs

- Reseeding of passive replicas
- Granular recovery of individual mailbox and public folder items with Single Mailbox Recovery (SMBR)

SnapCenter Plug-In for Microsoft Windows

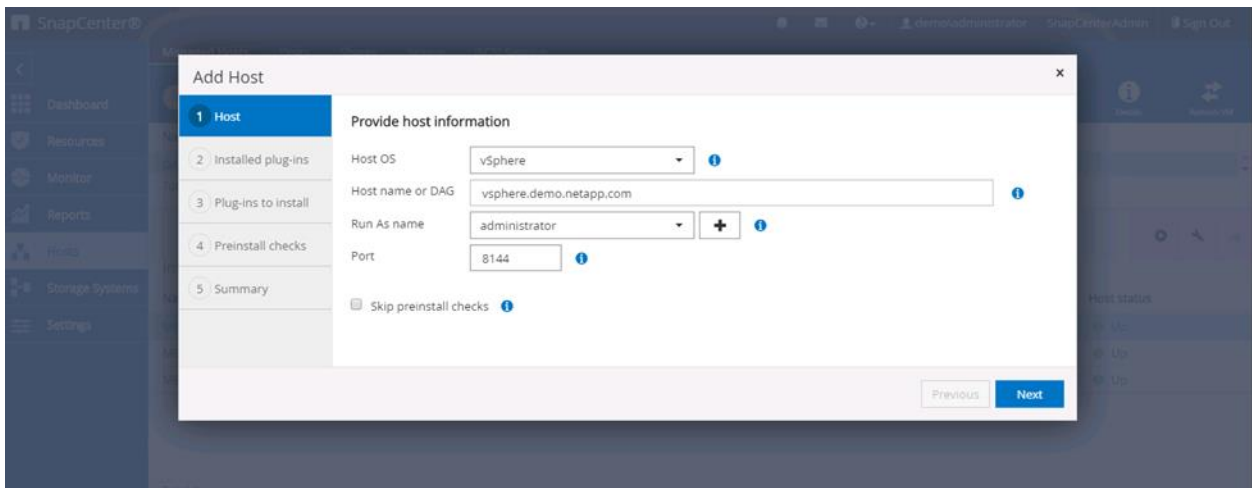
The NetApp SnapCenter Plug-In for Microsoft Windows (SCW) is a host-side component that integrates with NetApp Snapshot technology. It manages disks in both physical and virtual environments, making LUNs available as local disks on Exchange hosts. SCW provisions 64,000 storage disks, enables Snapshot copy consistency and space reclamation, initiates iSCSI sessions, manages igroups, and performs backup and restore operations on Exchange hosts. Note the following key features of SCW:

- Creates space-efficient backups of Exchange environments
- Runs multiple backups at the same time across multiple servers
- Provides PowerShell cmdlets for scripting of backup and restore operations
- Enables enhanced online storage configuration, LUN resizing, and streamlined management

SnapCenter Plug-In for VMware vSphere

SnapCenter interacts with the SnapCenter Plug-In for VMware vSphere (SCV) to support backup and restore of Exchange databases on raw device mappings (RDMs). To use SCV, you must register the VMware vSphere server with the SnapCenter Add Host wizard as shown in Figure 4.

Figure 4) Register VMware vSphere in SnapCenter.



Best Practices

- To enable data protection for Microsoft Exchange, make sure that SnapManager Suite or a SnapCenter Standard controller-based license is available on the ONTAP storage system through a Premium or Flash bundle.
- Make sure that the SnapCenter Plug-Ins Package for Windows is installed on an Exchange server that has at least 1GB of RAM, although 8GB is recommended. Also, see the [Exchange 2016 system requirements](#).
- To protect the Exchange databases, verify that the SnapCenter Plug-Ins Package for Windows is installed on a stand-alone Exchange server or members of the DAG.
- The SnapCenter Plug-Ins Package for Windows and the SnapCenter Plug-In for Microsoft Exchange Server must be the same version, because SCE uses the VSS Hardware Provider in SCW.
- Make sure that SnapCenter Plug-Ins Package for Windows version 4.1 is installed on the hosts to fully take advantage of all the data protection features of SnapCenter.
- To provision and resize RDM LUNs connected by an FC or iSCSI host bus adapter (HBA), you must use PowerShell cmdlets.

2.2 Role-Based Access Control in SnapCenter

SnapCenter uses RBAC to delegate functionality to application and database owners while retaining oversight and control by a central storage infrastructure administrator. This level of control and security frees storage administrators from performing tedious tasks that application and database owners can do for themselves. At the same time, it protects the overall infrastructure from bullying applications and from accidental infrastructure abuse by users. SnapCenter provides application-specific or database-specific workflows tailored to meet the needs of application, database, and virtualization infrastructure administrators.

What you see depends upon your settings in the SnapCenter RBAC. You can assign your Exchange database administrators (DBAs) to see only hosts, storage systems, and policies related to Exchange, whereas your SQL DBAs can see only assets and information related to SQL Server. Configuring RBAC for users is a two-step process in the settings. This process enables users to perform the actions for which they have permissions on the assets that are assigned to them. You can create and modify roles and add resource access to users at any time.

- **Roles.** SnapCenter has predefined roles with specific permissions assigned to the role to which you can add users or groups. You also can create roles.
- **User access.** Assign the user access to SnapCenter assets, such as hosts and storage connections.

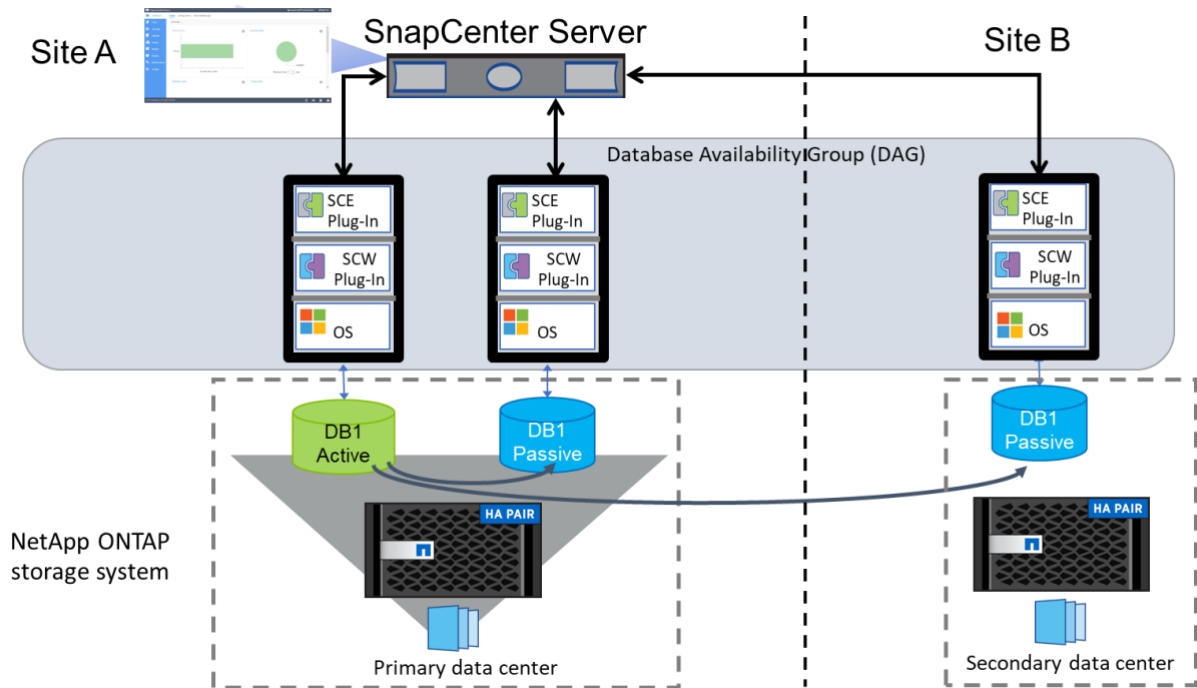
Best Practices

- RBAC users should have plug-in install and uninstall permission, such as the SnapCenter administrator role, so that they can deploy the plug-in successfully on Exchange hosts.
- When logged in as an RBAC user, click Refresh Resources in the Resources window so that Exchange resources display correctly.

2.3 SnapCenter Plug-In for Microsoft Exchange Server Architecture

SnapCenter coordinates interactions among the SnapCenter Server, Exchange hosts, and ONTAP systems to create and manage application-consistent Snapshot copies of Exchange databases. SnapCenter uses the VSS feature of Windows Server for point-in-time or up-to-the-minute restore.

Figure 5) SnapCenter data protection of a Microsoft Exchange Database availability group.



2.4 SnapCenter Plug-In for Microsoft Exchange Server Installation and Upgrade Considerations

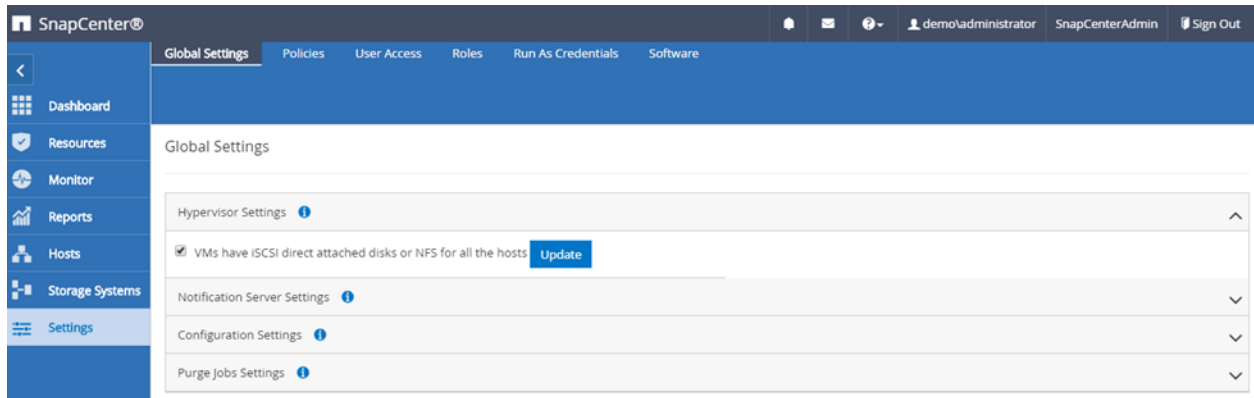
An upgrade or migration from earlier versions of NetApp SnapManager for Microsoft Exchange Server (SME) to SnapCenter is not available. Although they can coexist in a side-by-side installation, you cannot use SnapCenter to restore databases from Snapshot copies created by SME.

Before upgrading to SnapCenter, you should complete the following steps:

- Back up the operating system installation on Exchange Server, including all the server system-state information—the registry, the boot files, and the COM+ class registry.
- Back up the data on local drives on Exchange Server.
- Back up the boot and system drives.
- Use your backup utility to create and maintain a current emergency repair disk.

Note: In VMware environments, you must update your hypervisor settings so that SnapCenter no longer displays a Configure Hypervisor message for overall status on the Add Host page. This message occurs when your Exchange Server environment is using an iSCSI initiator.

Figure 6) SnapCenter hypervisor settings.



Best Practices

- Before you install the SnapCenter Plug-Ins Package for Windows, make sure that all Exchange host system prerequisites are met and the Exchange host is restarted so that the Validate in Preinstall function checks the prerequisites correctly.
- If you are using a DAG, select Add All Hosts in the cluster or DAG.
- Refer to the [NetApp Interoperability Matrix Tool \(IMT\)](#) for version compatibility between SnapCenter Server and any plug-ins.
- When SCE coexists with SME, SnapDrive for Windows and SCW both contain VSS Hardware Providers that cannot be used simultaneously, because they both claim disks on the Exchange server. This conflict can cause issues in data protection. Verify that Data ONTAP VSS Hardware Provider for SnapCenter (version 7.0.0.5561) is registered.
- For Exchange databases in a VMware environment, verify that SCV is also upgraded. After a successful upgrade, clear the browser cache before running any plug-in for VMware vSphere operations, because some operations might hang.

2.5 SnapCenter Plug-In Uninstall Considerations

If you no longer need a particular SnapCenter plug-in, you can uninstall it using the SnapCenter interface. Uninstalling the SnapCenter Plug-Ins Package for Windows from the Exchange host automatically removes the resources or resource groups, policies, and backups associated with the resource groups. Uninstalling also unregisters with vCenter when you use SCV. If you uninstall the plug-ins individually, uninstalling the SCE plug-in automatically uninstalls the SCW plug-in as well. Unless you are certain that you no longer require SnapCenter Server, do not uninstall the SnapCenter Plug-Ins Package for Windows from the SnapCenter Server, Uninstalling damages SnapCenter Server installation.

Note: Before you reinstall the plug-in on a host, wait 5 minutes so that the SnapCenter GUI refreshes the status of the managed host.

Best Practices

- NetApp recommends uninstalling SnapCenter plug-ins from the SnapCenter GUI. Otherwise, the data associated with the Exchange host is not deleted.

3 Storage Layout Planning

Planning and designing the storage layout is the most critical step for Exchange environments. This step has a direct impact on the availability of Microsoft Exchange and reduces the administrative overhead associated with managing the volumes hosting Exchange data.

3.1 Aggregate

Creating separate aggregates for Exchange database and transaction log volumes can meet the performance requirements while providing the data availability required by typical SLAs.

Consider the following issues:

- Place Microsoft Exchange Server workloads on an individual aggregate to allow isolation from other I/O-intensive applications and workloads.
- For optimal storage performance, NetApp recommends thin provisioning and having at least 10% free space available in an aggregate hosting Exchange data.
- NetApp strongly recommends setting the autodelete trigger to volume.
- Place flexible volumes for active and passive copies of each database in a DAG onto separate aggregates. If a single aggregate is lost, only the database copy on that aggregate is affected.

3.2 Volumes

The number of volumes you provision depends on your backup strategy. If your recovery time objective (RTO) is very small, it is best to place each database on its own database and transaction log volumes. In high-availability architectures, there are two possibilities for volume layout:

- A single database per volume (database and corresponding log files are placed on the same volume)
- Multiple databases per volume

Also, the restore mechanism depends on the volume layout containing the Exchange databases.

Note: NetApp SnapCenter does not support active and passive replicas on the same volume.

Best Practices

- Isolate Windows Server files and Exchange application files onto separate volumes to improve performance.
- NetApp recommends separating database (random I/O) and transaction logs (sequential I/O) into separate volumes or physical disks. Doing so maximizes hard disk I/O performance and increases fault tolerance. If the disk that contains the database files is damaged, you can use the latest backup and all the transaction log files. The backup can be used to recover all of the Exchange data.
- Move write-intensive non-Exchange workloads onto volumes separate from those containing Exchange databases.
- Design identical storage in terms of capacity and performance for active and passive copies of the mailboxes.
- Isolate each DAG replica onto separate volumes on separate disks to avoid a single point of failure.
- NetApp recommends enabling read reallocation (`read_realloc`) on NetApp FlexVol® volumes hosting Exchange databases. Doing so improves read performance for Exchange workloads with a mixture of large sequential reads and random writes.
- Do not create mount points for LUNs that hold an Exchange database or create any files or folders in the root folder where the mount points are created. The restore operation removes any mount points that were created after the backup, disrupting access to the data on the mounted volumes referenced by these volume mount points.
- Do not place databases or transaction logs on a mount point root volume.

3.3 LUNs

Optimizing disk I/O is one of the largest performance-enhancing considerations for Microsoft Exchange. Database LUNs can be optimized for random reads and writes, and transaction log LUNs can be optimized for sequential writes because logs are always written to and read from sequentially. Also, the number of LUNs you provision depends on your SLA requirements and recoverability defined by the recovery point objective (RPO) and the RTO.

One LUN per Database

Both the database (.edb) and its corresponding log files (.log) are placed on the same LUN. Although this configuration simplifies storage administration because there are fewer LUNs to manage, this configuration creates a single point of failure. Therefore, the mailbox database must be configured as a part of a DAG with two or more copies to make sure that you can recover your database if a failure occurs.

Two LUNs per Database

The mailbox database (.edb) and transaction log (.log) are placed on separate LUNs (each on a separate volume) to provide the best RPO and RTO. Although this approach increases the total number of LUNs required, volume mount points can be used because there are a finite number of drive letters available. NetApp recommends limiting the number of log streams per LUN to between 5 and 10.

Best Practices

- Provision the active and passive LUNs so that they are identical in path, capacity, and performance.
- In a DAG, each database path must be the same on every DAG node that has a copy of that database. Therefore, use volume mount points when creating LUNs.
- Use larger databases. Microsoft supports databases up to 16TB in size, with a best practice size of 2TB.

3.4 Capacity Planning

A properly sized Exchange environment meets both Microsoft requirements for Exchange storage and any requirements indicated in customer SLAs. For an environment to be properly sized, information from the customer environment is collected and tools are used to convert that information into a physical storage recommendation.

When planning an Exchange environment for a customer, use the following tools:

- The Microsoft Exchange Server role requirements calculator
- The NetApp Exchange sizing tool

When sizing Exchange Server deployments that use NetApp storage, it is important to use the NetApp Exchange sizing tool with data from the Microsoft Exchange Server role requirements calculator.

Best Practice

- Consult a local NetApp Exchange expert or your NetApp partner to help size Exchange Server accurately. Use the NetApp sizing tool for Exchange to size all Exchange Server deployments that use NetApp storage.

3.5 Data Protection

SnapCenter enables data protection for your Exchange environments, and you must invest significant time for planning so that you understand how data is protected according to your organization's needs.

Backup

It is important to understand business drivers like the SLA, RTO, and RPO before you determine your backup strategy. The RTO indicates how long you can afford to go without access to Exchange if an outage occurs, whereas the RPO is a measure of how much data you can afford to lose.

Planning the backup strategy for Exchange databases 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.

Use the following points to guide your backup strategy:

- Determine the number of Exchange servers, DAGs, databases, the size of the database, network links, and so on.
- Understand SLAs, RPOs, and RTOs.
- Decide the type of backup you require.
- Determine when you should back up your databases.
- Decide how many backup jobs you require.
- Decide how to name your backups.
- Determine how long you want to retain backup copies on the source and destination storage systems.

- Determine how long you want to retain transaction log backups on the source and destination storage systems.

SnapCenter introduces portable backup of Microsoft Exchange resources to replace the SME gapless backup feature. For this feature, the backup of a mailbox database can be offloaded to one or more replica copies instead of backing up all replicas (active and passive). This portable backup of the replica copy can be used to perform point-in-time or up-to-the-minute restore of the active copy on any failed DAG node in the same organization. This mechanism helps conserve storage space and reduces the backup Snapshot management overhead. SnapCenter backups provide a recovery mechanism in the rare event of systemwide, catastrophic logical corruption or administrative error, so you don't need to keep a lagged copy in the DAG.

Note the following:

- A backup of a DAG database from a physical server through iSCSI cannot be used to restore a VMware virtual machine with RDM disks and conversely.
- SnapCenter data protection of Exchange databases through the Resilient File System (ReFS) is not supported. If you have a business need or use case for ReFS, email ng-snapcenter-feedback@netapp.com.
- SnapCenter data protection of an Exchange database on Bitlocker encryption-enabled drives is currently not supported.

In the DAG settings of a new Exchange Server backup policy, you can choose either to back up active copies or to back up copies on servers that you'll select when you create a backup job.

New Exchange Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Summary

Select Exchange server backup options

Choose backup type

Full and Log backup

Full backup

Log backup

Copy Backup

Database Availability Group Settings

Select one or both options

Back up active copies

Back up copies on servers to be selected during backup job creation time

Schedule frequency

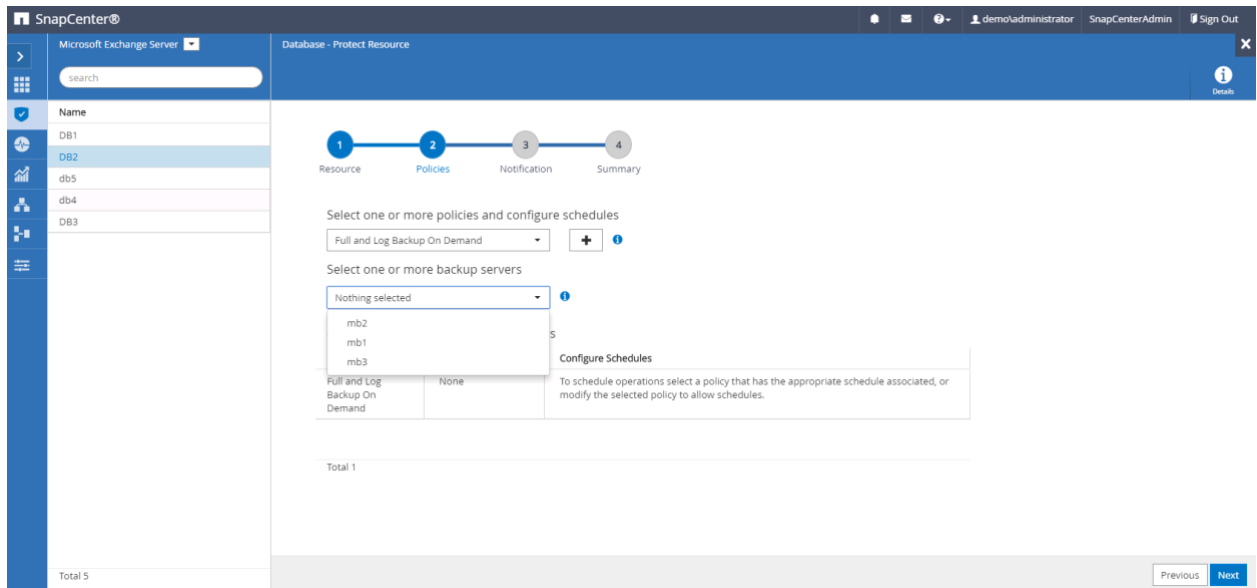
Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

Hourly

Daily

Previous Next

If you select Back Up Copies on Servers to Be Selected During Backup Job Creation Time, you can select the server on which the backup should run.



SnapCenter 4.1 introduces copy backup, which backs up all selected databases and their logs without log truncation.

Note: Copy backups provide an image of data for use in testing and problem diagnosis or for seeding a replica. They are not intended for data recovery.

In previous versions of SME, the latest Snapshot copy ended with `_recent`, which made it easy to write scripts to locate the latest Snapshot copies and move them to tape if necessary. To get the latest backup in SnapCenter, use the `Get-SmBackup` cmdlet as shown in the following screenshot.

```

PS C:\Users\Administrator.DEMO> Get-SmResources -HostName dag1.demo.netapp.com

cmdlet Get-SmResources at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
PluginCode: sce

Completed Discovering Resources: Job Id [297]

DBName       : DB3
ExchangeServer : MB3.demo.netapp.com
DAGName      : DAG1
DBId         : MB3.demo.netapp.com\DB3
Protected    :
ReplicaServers : MB1,MB2

DBName       : db4
ExchangeServer : MB2.demo.netapp.com
DAGName      : DAG1
DBId         : mb2.demo.netapp.com\db4
Protected    :
ReplicaServers : MB1,MB3

DBName       : db5
ExchangeServer : MB2.demo.netapp.com
DAGName      : DAG1
DBId         : mb2.demo.netapp.com\db5
Protected    :
ReplicaServers : MB3,MB1

DBName       : DB1
ExchangeServer : MB2.demo.netapp.com
DAGName      : DAG1
DBId         : mb2.demo.netapp.com\DB1
Protected    :
ReplicaServers : MB1,MB3

DBName       : DB2
ExchangeServer : MB2.demo.netapp.com
DAGName      : DAG1
DBId         : mb2.demo.netapp.com\DB2
Protected    :
ReplicaServers : MB3,MB1

PS C:\Users\Administrator.DEMO> Get-SmBackup -AppObjectName DB1

BackupId      BackupName      BackupTime      BackupType
-----
1             SCE_Resource Group for Exc... 2/22/2018 11:01:32 PM Full Backup
228          SCE_Resource Group for Exc... 3/4/2018 9:56:18 AM Full Backup
229          SCE_Resource Group for Exc... 3/4/2018 10:56:19 AM Full Backup
230          SCE_Resource Group for Exc... 3/4/2018 11:56:18 AM Full Backup
231          SCE_Resource Group for Exc... 3/4/2018 12:56:20 PM Full Backup
232          SCE_Resource Group for Exc... 3/4/2018 1:56:20 PM Full Backup
233          SCE_Resource Group for Exc... 3/4/2018 2:56:27 PM Full Backup
234          SCE_Resource Group for Exc... 3/4/2018 3:56:43 PM Full Backup

PS C:\Users\Administrator.DEMO> Get-SmBackup -AppObjectName DB1 | select -Last 1

BackupId      BackupName      BackupTime      BackupType
-----
234          SCE_Resource Group for Exc... 3/4/2018 3:56:43 PM Full Backup

```

SnapCenter 4.1 introduces support for replication of backup Snapshot copies to a secondary storage system by using NetApp SnapMirror and NetApp SnapVault. This process can be defined in the Exchange Server backup policy.

Note: Cascade relationships are not supported.

New Exchange Server Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Summary

Select secondary replication options i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label i One Time

Error retry count 3

One Time

Hourly

Daily

Weekly

Monthly

Custom Label

Previous
Next

Best Practices

- Verify that Microsoft VSS and VSS Writer are enabled on the Exchange server so that you can protect the Exchange environments by using SnapCenter.
- Back up Exchange data regularly depending on the backup strategy that best meets your recovery objectives. This approach reduces the amount of space required to restore your Exchange databases, because full backups delete the transaction log files up to the time that you perform the backup. With this strategy, you do not have to restore more than one day's worth of log files.
- Verify that all copies in the DAG are in a healthy state.
- Keep the active and passive databases on separate volumes so that the SnapCenter backup does not fail, indicating that a Snapshot copy with a name already exists on the layout.
- Verify that circular logging is disabled for each database being protected by SnapCenter so that you can recover data up to the minute using the available transaction log.
- Keep Exchange databases at a manageable size according to Microsoft Exchange best practices; if databases are too large, backup and recovery times increase.
- Use OnCommand System Manager to configure relationships for SnapMirror and SnapVault. Otherwise, SnapCenter backups fail with a warning. You cannot create relationships by using SnapCenter.
- The primary and secondary SVMs must be registered with SnapCenter and assigned to the same specific RBAC user responsible for data protection.
- SnapCenter Server and Exchange hosts should have necessary connectivity to the primary and secondary storage systems.

Snapshot Retention Guidelines

SnapCenter backup operations work as follows:

- SnapCenter creates a VSS backup of the Exchange database, which gets deleted according to the full backup retention settings.
- To enable up-to-the-minute restore, SnapCenter archives transaction logs to the `SceBackupInfo` directory by creating NTFS hard links to the live transaction log files without physically copying the log file. This archived transaction log is deleted as a part of log backup retention.

Figure 7) Log and full backup retention settings.

The screenshot shows the 'Modify Exchange Server Backup Policy' window with a sidebar on the left containing six steps: 1 Name, 2 Backup Type, 3 Retention (selected), 4 Replication, 5 Script, and 6 Summary. The main content area is titled 'Retention settings' and is divided into two sections. The first section, 'Log Backup retention settings for up-to-the-minute restore operation', has two radio button options: 'Number of full backups for which logs are retained' (selected) with a text input field containing '7', and 'Keep log backups for last' with a text input field containing '14' and a 'days' button. The second section, 'Full backup retention settings', has a dropdown menu currently showing 'On demand' with a downward arrow, and 'Hourly' is highlighted below it with an upward arrow. Below the dropdown are two radio button options: 'Total Snapshot copies to keep' (selected) with a text input field containing '7', and 'Keep Snapshot copies for' with a text input field containing '14' and a 'days' button. At the bottom right of the window are 'Previous' and 'Next' buttons.

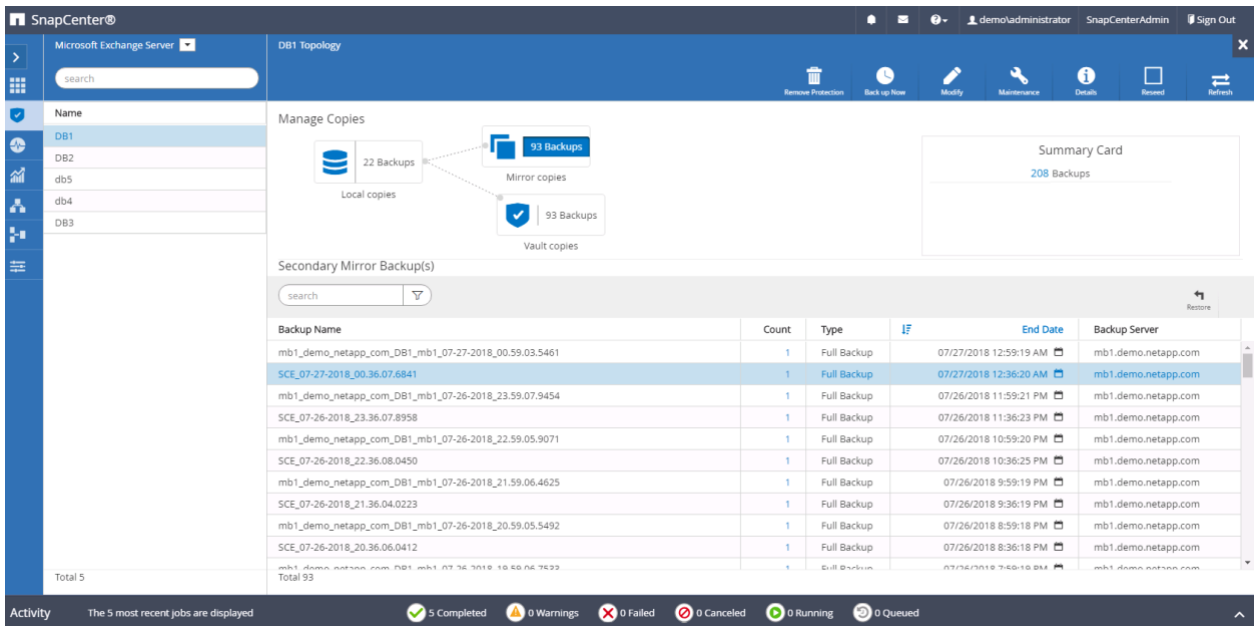
NetApp flexible volumes running NetApp ONTAP can store a maximum of 255 Snapshot copies per flexible volume. The amount of storage needed for NetApp Snapshot copies depends on the change rate. To provide accurate volume sizing and layout for Exchange environments, consult a NetApp Exchange expert or your NetApp partner.

Best Practice

- A database and its corresponding transaction log must be placed on separate LUNs if you want to use separate backup and retention schedules.

Restore Guidelines

The topology displays local, mirror, and vault copies from which you can perform the restore operation.



There are two types of restore operations:

- **Up to the minute.** An up-to-the-minute restore mounts the database, and Exchange replays the transaction logs from the backup and applies them to the database. The complete transaction log chain is required for an up-to-the-minute restore to succeed. To restore all the available log backups after the full backup, choose All Log Backups.
- **Point in time.** This option allows you to restore your Exchange data to a chosen point in time. Any Exchange data past that point is not restored. This option is particularly useful when you want to restore to a point before an event such as data corruption occurred. A point-in-time restore replays and applies to the database only those transaction logs that existed in the active file system when the backup was created up to the specified point in time. All transaction logs beyond that point in time are discarded.

Choose By Log Backups Until to restore the database based on the backup log with the selected date. Choose By Specific Date Until to specify the date and time after which transaction logs are not applied to the restored database. The point-in-time restore operation halts the restoration of transaction log entries that were recorded after the specified date and time. Choose None when you need to restore only the full backup without any log backups.

Figure 8) SnapCenter restore options.

The technology that you use for a restore depends on the storage layout of the database in the volumes, as shown in Table 1.

Table 1) Restore options.

Storage Configuration	Primary	Secondary
Single database scenario: <ul style="list-style-type: none"> Eg: DB1 E: db1.edb T: db1.log 	Perform a single-file SnapRestore (SFSR) restore of the LUN.	Perform a SnapMirror restore (SFR). This restore is most efficient because the storage network, not the host network, is used, with only the incremental delta of the LUN restored from secondary storage.
Multiple databases: <ul style="list-style-type: none"> Eg: DB1, DB2 E: db1.edb, db2.edb T: db1.log, db2.log 	By default, perform a sub-LUN restore. If restore fails, perform a mount and copy restore.	Perform a mount and copy restore.

After a successful backup, you might need to transition database ownership or the active node to another node. For example, during backup at time t1, node 1 owned the active copy, and later, because of a virus infection, a copy on node 2 was instantiated. Therefore, node 2 then owned the active copy. At this point, if you restore backup-t1, the restore must be performed for node 2. This requires mounting the database and log disks from the Snapshot copy on node 2 to perform the restore. Node 2 in this situation should have access to the controllers hosting the database and the log LUNs mounted on node 1. However, for a geographically separated cluster, this might not always be possible. Therefore, NetApp recommends that you back up the active or passive database copy in the remote data center to allow a successful restore.

Best Practices

- Verify that there is adequate hard disk capacity to restore both the database and the log files.
- Perform a test restore to an alternate Exchange server regularly to verify the backup consistency and success of the restore.
- For an up-to-the-minute restore, restore from your most recent full backup to minimize the number of transaction logs that must be replayed.
- Make sure that the storage from which the backup was taken is accessible to the target host where the restore is performed. Otherwise, the restore might fail.
- To verify the log's integrity, make sure to deselect Do Not Verify the Integrity of Transaction Logs in the Backup Before Restore. By default, the option is unselected.

Reseed Guidelines

When Microsoft Exchange Server runs in the DAG configuration, one of the replicas might go into a failed state, possibly because of corruption. If this occurs, you must recover the failed database copy by using the Microsoft Exchange Server reseed operation. Reseeding replicates data from the active database copy to the failed replica and brings this failed copy back to a healthy state. The time required for a reseed operation depends on the size of the database and on network performance. SnapCenter 4.1 makes DAG reseeding go many times faster, because a SnapCenter reseed operation uses NetApp Snapshot technology to restore from a backup Snapshot copy. This process has no effect on the active replica.

After SnapCenter reseeding restores the failed database copy to a healthy state, the latest content is available across all DAG copies because of replication from the active replica. Reseeding can be performed from backup Snapshot copies on the same node (default) or a different node. The storage network is used rather than host network resources.

The technology used for reseeding also depends on the storage layout of the database in the volumes, as shown in Table 2.

Table 2) Reseed options.

Storage Configuration	Reseed of FC/iSCSI/RDM (Same Node)	Reseed from Different Node
Single database scenario: <ul style="list-style-type: none">• Eg: DB1• E: db1.edb• T: db1.log	Volume SnapRestore restore	Mount and copy restore
Multiple databases: <ul style="list-style-type: none">• Eg: DB1, DB2• E: db1.edb, db2.edb• T: db1.log, db2.log	Single file SnapRestore (SFSR) restore. If SFSR fails, then mount and copy restore.	Mount and copy restore

Best Practices

- Create a backup or select the most recent backup Snapshot copy across the nodes, because the lag between the active copy and passive copy to be recovered is minimal. This process also affects the time taken for the reseed operation.
- Verify that there is connectivity between the reseed target node and the storage containing the backup Snapshot copy.

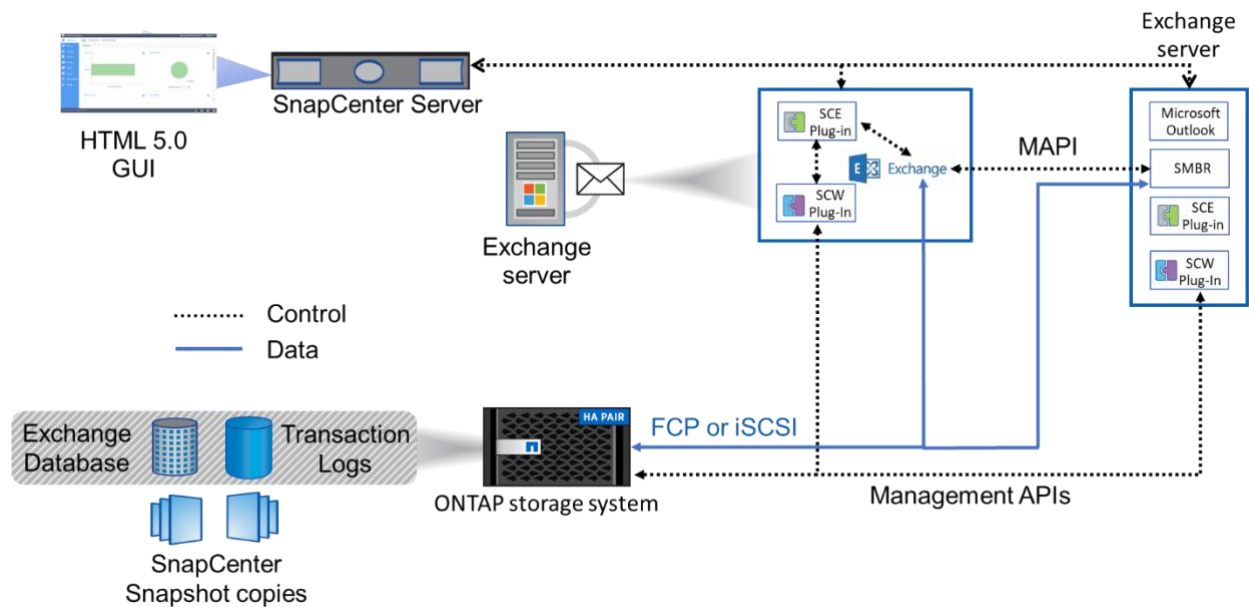
Single Mailbox and Item-Level Recovery

NetApp SMBR software can be used for the following functions:

- Repairing accidental or malicious deletion of items.
- Rapidly recovering Exchange data directly to your production Microsoft Exchange Server or any PST file at any level of granularity, including individual mailboxes, public folders, messages, attachments, calendars, notes, and tasks.
- Using near-instantaneous online backups of Exchange databases created with SnapCenter. This eliminates time-consuming and expensive single mailbox (brick-level) backups and the need for a recovery server.
- Searching for and creating a copy of all archived emails that match a given keyword or other criteria.

SMBR runs on the Exchange server on which Microsoft Outlook is running and the SnapCenter Plug-Ins Package for Windows is installed. SMBR uses the native Microsoft Messaging Application Program Interface (MAPI) protocol to communicate with the Exchange server that is running on a separate machine.

Figure 9) Single Mailbox Recovery architecture.



Note: You can request a trial license by sending your name, your company's name, and your email address to GlobalDSTTechSupport@kroll.com.

For a permanent license, open a NetApp license support case to check the customer license entitlement. The entitlement is based on the bundle (Premium or Flash) and any add-on purchases.

Microsoft Outlook must be installed and configured to a mailbox on the Exchange server. However, you do not need to run it continuously on the Exchange server.

4 NetApp Storage Efficiency

Storage efficiency is the ability to store and manage Exchange Server data in a way that consumes the least amount of storage space, with little or no impact on the overall performance of the system. To design an efficient storage solution, you must understand the I/O and bandwidth characteristics of Microsoft Exchange. Typically, Exchange databases encounter 32KB random reads to the database and sequential writes for the transaction log, which typically vary from 4KB pages (the native I/O size) to a log buffer size of 1MB. Storage efficiency goes beyond data deduplication; it is a combination of provisioning (overall layout and utilization) and data protection technologies.

Storage Efficiency	Best Practice
NetApp Snapshot technology	This feature provides zero-cost, fast-backup, point-in-time copies of the volumes hosting Exchange databases.
Thin provisioning	Use thin-provisioned volumes for the Exchange databases and logs.
Space reclamation	Space reclamation should be run during periods of low activity because it initially consumes cycles on the host.
Fractional reserve	The default value for the fractional reserve is 100%. However, by using the autodelete feature, the fractional reserve can be set to 0.
Autodelete	NetApp recommends setting the autodelete trigger to volume.
Autogrow	There must be enough space available in the aggregate for the autosize option to function. NetApp recommends planning for additional buffer space when you use thin provisioning for Microsoft Exchange Server environments.
Deduplication	NetApp recommends deduplication for database volumes, but not for transaction log volumes. Turn on scheduled deduplication and schedule it for nonpeak hours (typically late at night).

5 Performance

Providing good performance to meet Exchange service levels depends on the proper sizing of NetApp storage for Exchange workloads.

Best Practices

- Use [System Performance Modeler \(SPM\)](#) to correctly size Exchange environments that use the [Exchange Server Role Requirements Calculator v9.1](#) as input. For more information, see [NetApp System Performance Modeler and Microsoft Exchange Server 2016 and 2013](#).
- Consult a local NetApp Exchange expert to provide accurate performance sizing and layout for Exchange environments.

5.1 SATA Performance Considerations

If you have an SATA-based deployment of Exchange, consider that SATA drives have a lower I/O profile than SAS and FC drives. NetApp Flash Cache™ intelligent caching can be used to help improve the I/O performance and reduce latency of SATA-based deployments. NetApp recommends Flash Cache and SATA if deployments exceeding 1,000 mailboxes or if SATA-based designs are bounded by performance instead of capacity.

Best Practice

- Have fewer, large databases to help reduce the complexity of the storage design and amount of background maintenance I/O, which can exceed the transactional I/O generated by users.

6 Virtualization

Virtualizing Exchange environments can deliver significant benefits, including reduced server hardware costs, reduced power usage, greater space savings, improved server utilization, and rapid server provisioning.

Best Practices

- NetApp recommends separating Exchange roles onto different servers so that no particular role fails if a host server fails.
- Separate Exchange data storage from the storage that hosts the guest virtual machine's operating system.
- Make sure that a similar storage configuration is used on every node in the DAG.

7 High Availability

A DAG is used for data resiliency by deploying multiple copies of mailbox databases across the two data centers. This configuration protects mailbox data from software, hardware, and even data center failures. The overall design of the DAG, the number of DAG members, and the number of mailbox database copies depend on your recovery SLAs for RTO and RPO. A larger DAG provides more redundancy and resources. NetApp SnapCenter enables point-in-time or up-to-the-minute restores, without the added capacity requirements and complexity of a lagged copy.

Best Practices

- Place the database replicas in a consistent, distributed configuration to make sure that they are evenly distributed after a failure.
- To avoid a single point of failure, verify that the replicas of a specific mailbox database are not placed in the same server rack or storage array.

8 Disaster Recovery

A DAG that relies on transaction log shipping for data replication can be extended to multiple sites to provide resiliency against disk, server, network, and data center failures. When a single server or database is lost, the DAG automatically performs switchover to activate the database copies on the other DAG nodes to keep Exchange services online.

Recover Microsoft Exchange Server and use NetApp SnapCenter to set up the network connections to the NetApp ONTAP storage system. In addition, connect to the database and transaction log LUNs for the Exchange database to recover from the most recent backup.

9 Summary

Microsoft Exchange Server is not a one-size-fits-all application. Multiple configuration options are available to suit most of a customer's needs. NetApp storage and data management software is built in a similar fashion, so that users can manage Exchange data to meet their business requirements. With high-performance, easy-to-manage storage systems and robust software offerings, NetApp offers the flexible storage and data management solutions to support Exchange Server 2013 and 2016 enterprise messaging systems.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents:

- SnapCenter 4.0 Concepts Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2840878
- SnapCenter 4.0 Data Protection Guide for Microsoft Exchange Server
https://library.netapp.com/ecm/ecm_download_file/ECMLP2840889
- SnapCenter 4.0 Administration Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2840880

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.

Copyright Information

Copyright © 2018 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.