



SnapManager® 7.2.1 for Microsoft® Exchange Server

Installation and Setup Guide

For Clustered Data ONTAP®

April 2020 | 215-13145_B0
doccomments@netapp.com

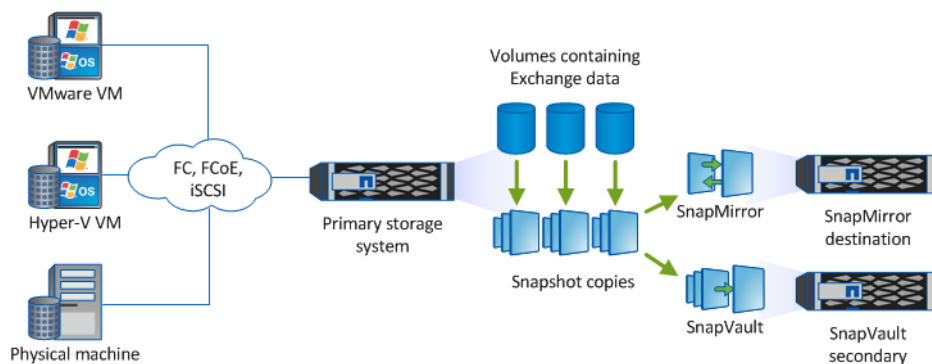
Contents

Product overview	4
Deployment workflow	6
Preparing for deployment	7
Storage layout requirements	7
SnapManager dedicated servers	9
SnapManager licensing	9
Supported configurations	10
Supported storage types	11
Windows host requirements	12
Service account requirements	13
Installing SnapManager	16
Installing SnapManager interactively	16
Installing SnapManager from the command line	17
Migrating databases to NetApp storage	19
Connecting SnapManager to Exchange Servers	19
Migrating databases and configuring SnapManager for Exchange servers	20
Preparing storage systems for SnapMirror and SnapVault replication	23
Understanding the differences between SnapMirror and SnapVault	23
Preparing storage systems for SnapMirror replication	24
Preparing storage systems for SnapVault replication	25
Backing up and verifying your databases	28
SnapManager backup overview	28
Defining a backup strategy	28
Backing up your databases for the first time	31
Verifying the initial backup set	33
Scheduling recurring backups	33
Scheduling frequent recovery point backups	34
Scheduling recurring backup set verifications	35
Where to go next	36
Copyright	37
Trademark	38
How to send comments about documentation and receive update notifications	39
Index	40

Product overview

SnapManager for Microsoft Exchange Server is a host-side component of the NetApp integrated storage solution for Microsoft Exchange, offering application-aware primary Snapshot copies of Exchange databases. You can use SnapManager with Data ONTAP SnapMirror technology to create mirror copies of backup sets on another volume, and with Data ONTAP SnapVault technology to archive backups efficiently to disk.

Together these tools offer a complete Snapshot-based data protection scheme that is as scalable, reliable, and highly available as the underlying storage system. The following illustration shows the components in a SnapManager deployment:



SnapManager highlights

SnapManager features seamless integration with Microsoft products on the Windows host and with NetApp Snapshot technology on the back end. It offers an easy-to-use, wizard-based administrative interface.

- *Integration with the Microsoft Volume Shadow Copy Service (VSS)* ensures that write requests are frozen and write caches are flushed before backups are taken. SnapManager supports Windows Volume Manager, Windows Server Failover Clustering, Microsoft Multipath I/O (MPIO), and Exchange Database Availability Groups.
- *Fast, nondisruptive Snapshot technology* using NetApp SnapDrive for Windows software enables you back up databases in seconds and restore them in minutes without taking Exchange Servers or databases offline. Snapshot copies consume minimal storage space. You can store up to 255 copies per volume.
- *Automated central administration* offers hands-off, worry-free data management. You can schedule routine Exchange Server database backups, configure policy-based backup retention, set up point-in-time and up-to-the-minute restore operations and proactively monitor your Exchange Server environment with periodic email alerts. PowerShell cmdlets are available for easy scripting of backup and restore operations.

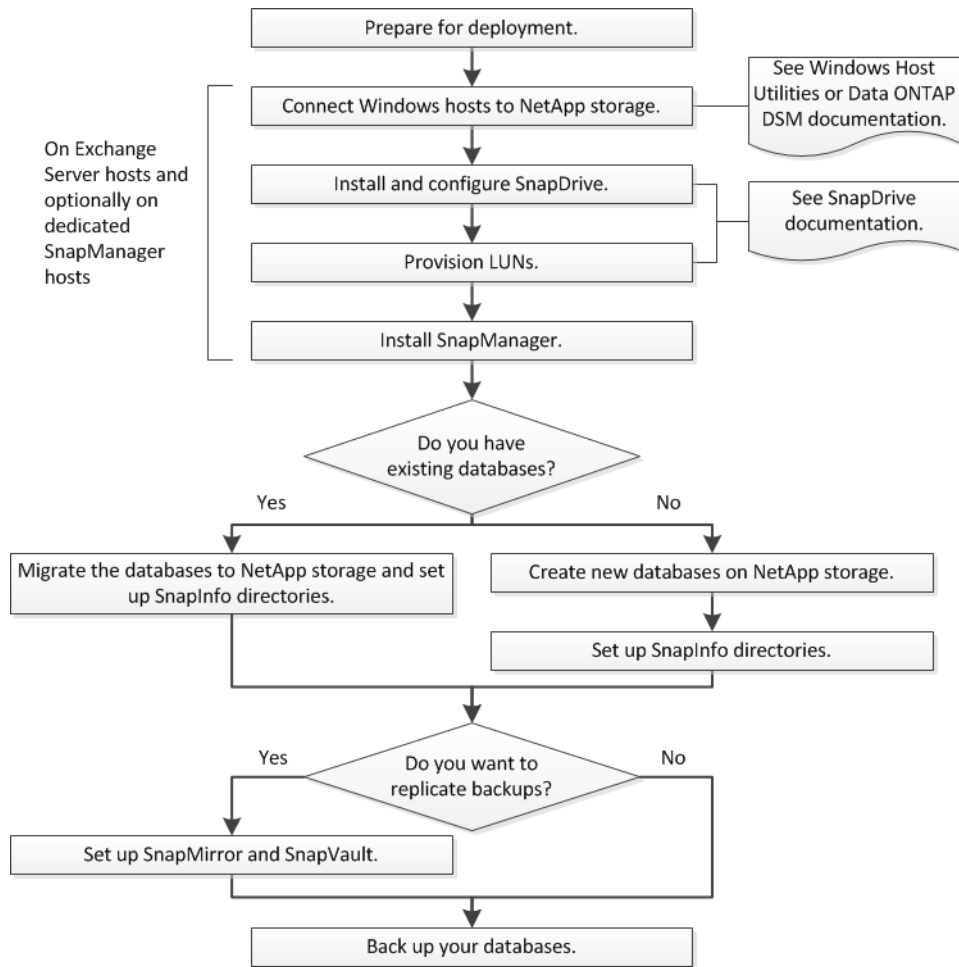
In addition to these major features, SnapManager offers the following:

- Integrated Single Mailbox Recovery enables you to restore individual mailboxes, email messages or attachments, calendar items, deleted items, drafts, or contacts (Single Mailbox Recovery must be installed separately)
- Simplified migration of existing databases to NetApp storage with an easy-to-use Configuration wizard

- Nondisruptive, automated backup verification
- Fast reseeding of databases in a Database Availability Group
- Support for physical and virtualized infrastructures
- Support for iSCSI, Fibre Channel, and FCoE
- Support for service-level Role-Based Access Control (RBAC)

Deployment workflow

Before you can create backups with SnapManager, you need to install the SnapDrive for Windows and SnapManager software, and provision NetApp storage. You can then migrate your databases to the storage system or create new databases in the system.



Preparing for deployment

Before you deploy SnapManager, you need to determine your storage layout, choose a SnapManager configuration, verify that you have the required licenses, and make sure that your Windows hosts meet the minimum requirements.

Steps

1. Plan how to lay out your databases on NetApp storage.
2. Decide whether you are going to use a SnapManager dedicated server for administration or verification.
3. Verify that you have the required licenses.
4. Verify SnapManager support for your configuration and storage type.
5. Verify that your Windows hosts meet SnapManager requirements.
6. Set minimum permissions for the SnapManager service account.

Related references

[Storage layout requirements](#) on page 7

[SnapManager dedicated servers](#) on page 9

[SnapManager licensing](#) on page 9

[Supported configurations](#) on page 10

[Supported storage types](#) on page 11

[Windows host requirements](#) on page 12

[Service account requirements](#) on page 13

Storage layout requirements

A well-designed storage layout ensures that SnapManager can properly back up your databases and that you can meet your recovery objectives.

SnapManager backs up an Exchange database by creating Snapshot copies of database data files, transaction logs, and the SnapInfo directory it uses to store information about backed up files. You use the SnapManager Configuration wizard to create one or more SnapInfo directories when you migrate databases to NetApp storage.

Note: It is a best practice to use SnapDrive for Windows to provision storage. For all SnapManager best practices, see [NetApp Technical Report 4221: Microsoft Exchange Server 2013 and SnapManager for Exchange Best Practices Guide for Clustered Data ONTAP](#).

LUN setup

For each Exchange database, SnapManager requires that you configure the following:

- A LUN for database files (.edb), one database per LUN
You cannot store database files for multiple databases on the same LUN.
- A LUN for transaction logs (.log)
Logs for multiple mailbox databases can be stored on a single LUN as long as you limit the number of transaction log streams to 9 or less.

For storage efficiency reasons, most sites create the SnapInfo directory in the same LUN as transaction logs. In this configuration, SnapManager creates NTFS hard links when it archives transaction logs to the SnapInfo directory. Archiving transaction logs using hard links is almost always more efficient than performing a file copy.

You can store the SnapInfo directory on a different LUN if you think there is some risk you will run out of space. You cannot store the SnapInfo directory on the same LUN as database files.

Restrictions are as follows:

- You cannot store database files, transaction logs, or the SnapInfo directory on a SAN boot LUN or a LUN containing any other directories or files (including system paging files).
- You cannot store database files on a LUN that hosts NTFS volume mount points.

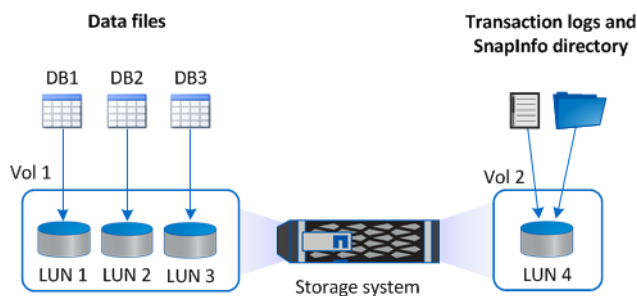
Volume setup

Snapshot copies are volume-wide, so you must be sure that items on the same volume have compatible backup schedules. Because Snapshot-copy contention issues can occur when databases from different Exchange Servers have different backup schedules, it is a best practice to store these databases on separate volumes. Similarly, because transaction logs are often backed up more frequently than database files, it is a best practice to store the database files and transaction logs for the same database on different volumes.

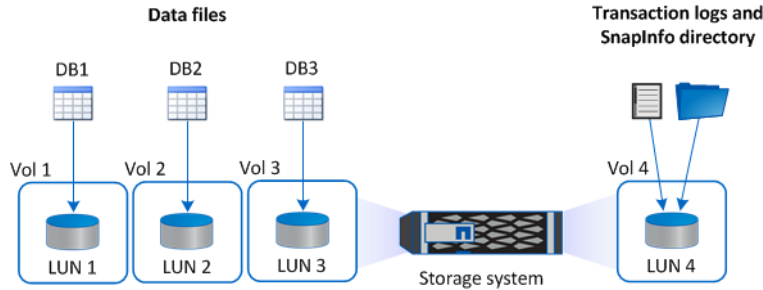
Ideally, you should store the database files and transaction logs for each database on a dedicated volume. This is the case even if the databases are from the same server. The following examples show the use of dedicated volumes:

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

You can store relatively small databases from the same server on a single volume as long as they have low transaction rates and your SLA does not require you to back up the databases frequently. In most cases, you can store transaction logs and the SnapInfo directory for each database on the same LUN, as shown in the following illustration:



The following illustration shows an ideal layout, in which the database files for each database are stored on different volumes:



SnapManager dedicated servers

Ordinarily, you install SnapManager on each Windows host running Exchange Server software with the mailbox role. From this *base configuration*, you can administer SnapManager locally or remotely. Depending on your needs, you might also want to install SnapManager on a dedicated administration or verification server.

- An *administration server* lets you manage SnapManager remotely from a host of your choosing. You might want to avoid using a primary Exchange Server host for SnapManager administration, or it might simply be more convenient to use a dedicated server.
- A *verification server* lets you offload backup set verification from a primary Exchange Server host.

SnapManager's optional backup set verification feature uses Exchange System Management Tools to check database and transaction log files for physical and logical corruption. Because verification is a CPU-intensive operation that can degrade Exchange Server performance, it is a best practice to run the utility on a dedicated server. The verification server must have iSCSI or FC connectivity with the storage system.

Verification is recommended in single node Exchange Server environments. Verification is not required for DAG databases that have at least two copies, each of which has a viable backup. For more information, see [NetApp KB Article 3013600: Does verification in SME need to occur in an Exchange 2010 DAG deployment?](#)

Tip: You can configure SnapManager to perform verification during or after backup. You can also configure it to verify the mirror or vault copy on the target storage system rather than the primary copy on the source system.

You can administer SnapManager from a verification server if it is more convenient than configuring a separate administration server.

SnapManager licensing

A SnapManager license and several storage system licenses are required to enable SnapManager operations. The SnapManager license is available in two licensing models: *per-server licensing*, in which the SnapManager license resides on each Exchange Server host, and *per-storage system licensing*, in which the SnapManager license resides on the storage system.

SnapManager license requirements are as follows:

License	Description	Where required
SnapManager per-server	A host-side license for a specific Exchange Server host. Licenses are required only for Exchange Server production hosts on which SnapManager is installed. No SnapManager license is required for the storage system or for the optional verification and administration servers.	On the SnapManager host. A SnapManager suite license is not required on source and destination storage systems when using per-server licensing.
SnapManager per-storage system (SnapManager suite)	A storage-side license that supports any number of Exchange Server hosts. Required only if you are not using a per-server license on the SnapManager host. Note: Trial licenses are available for per-storage system licensing only.	On source and destination storage systems.
SnapRestore	A required license that enables SnapManager to restore and verify backup sets. Restores include file level restores.	On source storage systems. Required on SnapMirror destination systems to perform remote verification. Required on SnapVault destination systems to perform remote verification and to restore from a backup.
FlexClone	An optional license for restoring an Exchange database to the Recovery Database.	On source storage systems.
SnapMirror	An optional license for mirroring backup sets to a destination storage system.	On source and destination storage systems.
SnapVault	An optional license for archiving backup sets to a destination storage system.	On source and destination storage systems.
Protocols	An iSCSI or FC license is required.	On source storage systems. Required on SnapMirror destination systems to serve data if a source volume is unavailable.

Supported configurations

You can use the NetApp Interoperability Matrix to verify SnapManager support for your configuration before you install or upgrade SnapManager.

The following table shows the currently supported software configurations:

Windows Server	Exchange Server	SnapDrive for Windows
2016 (Standard and Datacenter)	<ul style="list-style-type: none"> 2016 (Standard and Enterprise) with CU3 at a minimum 	Bundled
2012 R2 (Standard and Datacenter)	<ul style="list-style-type: none"> 2013 SP1 (Standard and Enterprise) 2016 (Standard and Enterprise) 	Bundled
2012 (Standard and Datacenter)	<ul style="list-style-type: none"> 2013 CU9 (Cumulative and Update) 2010 SP3 (Standard and Enterprise), with RU10 at a minimum 2016 (Standard and Enterprise) 	Bundled
2008 R2 SP1 (Standard and Enterprise)	<ul style="list-style-type: none"> 2013 SP1 (Standard and Enterprise) 2010 SP3 (Standard and Enterprise), with RU10 at a minimum 	Bundled

Related information

[NetApp Interoperability Matrix Tool](#)

Supported storage types

SnapManager supports a wide range of storage types on both physical and virtual machines. Verify support for your storage type before you install or upgrade SnapManager.

Machine	Storage type
Physical server	<ul style="list-style-type: none"> FC-connected LUNs iSCSI-connected LUNs
VMware VM	<ul style="list-style-type: none"> RDM LUNs connected via FC HBA RDM LUNs connected via iSCSI HBA iSCSI LUNs connected directly to the guest system by the iSCSI initiator
Hyper-V VM	<ul style="list-style-type: none"> Passthrough LUNs connected via FC HBA Virtual Fibre Channel (vFC) LUNs connected via virtual Fibre Switch Passthrough LUNs connected via iSCSI HBA iSCSI LUNs connected directly to the guest system by the iSCSI initiator

Windows host requirements

Windows hosts must meet the requirements for the base SnapManager configuration and for each of the optional dedicated SnapManager servers.

Important notes

- You can install SnapManager on any combination of physical machines or virtual machines.
- You must use the same version of SnapManager on all of the hosts.
- You should install SnapManager and SnapDrive for Windows on every Data Availability Group (DAG) member so that SnapManager can migrate all of the mailbox databases in the DAG and because doing so gives you the flexibility to back up Microsoft Exchange Server instances at the DAG level.
- You can connect the remote verification server to the storage system by using a different protocol from the protocol that you used to connect to the base configuration.

Host requirements per server type

The following table lists the host requirements for the base SnapManager configuration and for the optional administration and verification servers:

Requirement	Base	Administration	Verification	Notes
Exchange Management Tools	Yes	Yes	Yes	The version must match the version of Exchange Server that you are running on the primary hosts.
.NET Framework 4.5 or 4.6	Yes	Yes	Yes	
Windows Management Framework 4.0	Yes	Yes	Yes	Upgrading a Windows Server 2008 R2 SP1 host or Windows Server 2012 host to version 4.0 requires a reboot.
SnapDrive for Windows	Yes	Yes	Yes	Upgrading or installing a SnapDrive for Windows version that is supported by your version of Data ONTAP.

PowerShell Language Mode requirement

The PowerShell Language Mode for use with Exchange Server must be set to Full Language. Otherwise, you will receive an error when you generate SnapManager reports.

You can set the Language Mode in Internet Information Services (IIS) Manager on the Windows host (**Administrative Tools > Internet Information Services (IIS) Manager**).

In IIS Manager, you can access the Language Mode setting:

- In Exchange Server 2010, you can navigate to the Default Website (**Sites > Default Web Site**), then you can select **PowerShell > Application Settings > PSLanguageMode**.

- In Exchange Server 2013, you can navigate to the Exchange Back End Web site (**Sites > Exchange Back End**), then you can select **PowerShell > Application Settings > PSLanguageMode**.

In the **Edit Application Setting** dialog, you can enter FullLanguage in the **Value** field, then you can click **OK**.

You can restart IIS immediately (**Start > Run > IISReset**).

Port and connection requirements for Windows Firewall implementations

If you have enabled Windows Firewall on your hosts, TCP port 810 must be available (both inbound and outbound) for SnapManager communications, including communications with the optional verification servers and administration servers. For DAG support, SnapManager requires inbound connections to `SnapMgrService.exe`.

Related references

[SnapManager dedicated servers](#) on page 9

Service account requirements

A service account is a user account created explicitly to provide a security context for services running on Windows Server. You must specify a service account when you install or update a service. Before working with SnapManager, you must ensure that the SnapManager service account has the required permissions on the Windows host. There are no requirements for the Exchange Server service account.

The SnapManager service account must meet the following requirements:

- The account must be a domain user account
- The account must be a member of the Mailbox server's local administrators group
- The account must be assigned to one of the following Exchange Server management role groups:
 - The Exchange Organization Management role group
 - A custom management role group that allows all SnapManager operations or a subset, as described below

A management role group, which is a part of Exchange Server Role-Based Access Control (RBAC), grants SnapManager the ability to execute specific Exchange Server PowerShell cmdlets.

The Organization Management role group includes all of the required SnapManager permissions, but also includes many other tasks not required by SnapManager. If you need to restrict Exchange Server access to specific SnapManager operations, use a custom management role group instead.

If you use a custom management role group, you can grant permissions to all of the PowerShell cmdlets that SnapManager requires or a subset of the cmdlets. The following sections explain three common scenarios for setting up a custom management role group for SnapManager:

- [A role group that allows all SnapManager operations](#)
- [A role group that allows all SnapManager operations on a subset of databases](#)
- [A role group that allows database backups only](#)

Note: For more information about role groups, see [Microsoft TechNet: Create a Role Group](#) and [Microsoft TechNet: Understanding management role scopes](#).

A role group that allows all SnapManager operations

To allow all SnapManager operations, the SnapManager service account must belong to a custom management role group that contains role entries for the following:

- Add-MailboxDatabaseCopy
- Dismount-Database
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:\$true
- Mount-Database
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Remove-PublicFolderDatabase
- Restore-MailboxDatabaseCopy
- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:\$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

A role group that allows all SnapManager operations on a subset of databases

To allow SnapManager operations on a subset of databases, the SnapManager service account must belong to a custom management role group that contains the role entries listed in the previous section ([A role group that allows all SnapManager operations](#) on page 13).

In addition, a management scope that restricts access to the required set of databases must be assigned to the management role group.

Example

The following cmdlet creates a management scope that restricts user access to DB1 and DB2:

```
New-ManagementScope "SMEScope" -DatabaseRestrictionFilter {Name -eq 'DB1' -or Name -eq 'DB2'}
```

The following cmdlet assigns the management scope to the "SME" management role group, which restricts the users in that group to DB1 and DB2:

```
Get-ManagementRoleAssignment -RoleAssignee "SME" | Set-ManagementRoleAssignment -CustomConfigWriteScope "SMEScope"
```

A role group that allows database backups only

To allow database backups only, the SnapManager service account must belong to a custom management role group that contains role entries for the following:

- Get-AdServerSettings

- `Get-DatabaseAvailabilityGroup`
- `Get-ExchangeServer`
- `Get-MailboxDatabase`
- `Get-MailboxDatabaseCopyStatus`
- `Get-MailboxServer`
- `Get-PublicFolderDatabase`

Installing SnapManager

Ordinarily, you install SnapManager on each Windows host running Exchange Server software. Depending on your needs, you might also want to install SnapManager on a dedicated administration or verification server. You can use an interactive wizard or the command line to install the product.

Before you begin

- You should have backed up your Exchange databases.
- SnapDrive for Windows must be installed.

About this task

If you are backing up Exchange Servers at the DAG level, SnapManager must be installed on every node with a copy of the database. If you are backing up DAG members individually, SnapManager need only be installed on the nodes you plan to back up.

Related tasks

[Installing SnapManager interactively](#) on page 16

[Installing SnapManager from the command line](#) on page 17


Installing SnapManager interactively

You can use the SnapManager installation wizard to interactively install SnapManager on a Windows host.

Steps

1. Download the SnapManager for Exchange Server software from the NetApp Support Site.
[NetApp Downloads: Software](#)
2. Double-click the downloaded .exe file.
3. Complete the steps in the SnapManager installation wizard to install SnapManager.

Most of the fields in the wizard are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Account	<p>The user account that Windows uses to run SnapManager. This <i>SnapManager service account</i> must have specific permissions on the Windows host and the Exchange Server. For details, see Service account requirements on page 13.</p> <p>Specify the account name by using one of the following formats:</p> <ul style="list-style-type: none"> • <i>DomainName\UserName</i> • <i>UserName@DomainName</i> <p>Example:</p> 

Field	Description
License Type	The license type that you purchased, which is either per-server licensing or per-storage system licensing. For details, see SnapManager licensing on page 9. Leave the License Key field blank if you are using per-server licensing and would prefer to specify the license key in the SnapManager console.

Installing SnapManager from the command line

You can run the SnapManager installation program unattended, in silent mode, from the Windows command line.

Steps

1. Download the SnapManager for Exchange Server installer from the NetApp Support Site.
[NetApp Downloads: Software](#)
2. From a Windows command prompt on the local host, change to the directory where you downloaded the product installer.
3. Enter the following command at the command prompt:

```
installer.exe /s /v"/qn SILENT_MODE=1 [USERNAME=UserName]
[COMPANYNAME=CompanyName] [ISX_SERIALNUM=LicenseKey]
[INSTALLDIR=InstallDirectory] SVCUSERNAME=Domain\UserName
SVCUSERPASSWORD=Password SVCCONFIRMUSERPASSWORD=Password [/L*v DirPath
\LogFileName]"
```

Enter the following for each variable:

Variable	Description
<i>installer</i>	The name of the .exe file.
<i>UserName</i>	The name of the product administrator. If not specified, SnapManager retrieves the default value from the Windows registry.
<i>CompanyName</i>	The name of your company. If not specified, SnapManager retrieves the default value from the Windows registry.
<i>LicenseKey</i>	The per-server license key. Leave this field blank if you are using per-storage system licensing, or if you would prefer to specify the per-server license key in the SnapManager console. For details, see SnapManager licensing on page 9.
<i>InstallDirectory</i>	An alternate installation directory. If not specified, SnapManager uses the default directory: C:\Program Files\NetApp\SnapManager for Exchange
<i>Domain\UserName</i>	The user account that Windows uses to run SnapManager. This <i>SnapManager service account</i> must have specific permissions on the Windows host and the Exchange Server. For details, see Service account requirements on page 13.
<i>Password</i>	The password for the specified user account.
<i>DirPath\LogFileName</i>	The location and name of an installation log file, which is useful for troubleshooting. The asterisk (*) specifies that all installation information (such as status messages, non-fatal warnings, and error messages) should be logged.

Example

```
"SME7.1_x64.exe" /s /v"/qn SILENT_MODE=1 ISX_SERIALNUM=123  
SVCUSERNAME=mva\Administrator SVCUSERPASSWORD=examplepwd!  
SVCCONFIRMUSERPASSWORD=examplepwd! /L*V C:\SME_Install.log"
```

Migrating databases to NetApp storage

After you have provisioned NetApp storage with SnapDrive for Windows, you can migrate your databases to the storage system or create new databases in the system. In either case, you use the Configuration wizard to create the SnapInfo directory that SnapManager uses to store information about backed-up files.

Related tasks

[Connecting SnapManager to Exchange Servers](#) on page 19

[Migrating databases and configuring SnapManager for Exchange servers](#) on page 20

Connecting SnapManager to Exchange Servers

Before you can migrate your databases, you need to connect SnapManager to your Exchange Server.

Steps

1. From the Windows **Start** menu, click **SnapManager for Exchange**.

The SnapManager console opens and a message box informs you that you need to specify an Exchange Server.

2. Click **OK**.

The Add Exchange Server to be managed dialog box appears.

3. To select a server, double-click one in the list or click **Browse**.

If you have a Database Availability Group (DAG), you should connect to each DAG member and then to the DAG itself. While you can back up all databases from the DAG, you need to configure each individual DAG member using the SnapManager Configuration wizard.

4. After you select a server, click **Add**.

SnapManager connects to the server and then displays a message box, informing you that SnapManager for Exchange is not configured on the Exchange Server.

5. Click **OK**.

The Configuration wizard appears.

After you finish

Use the Configuration wizard to migrate databases to NetApp storage and to configure SnapManager for the Exchange Servers.

Migrating databases and configuring SnapManager for Exchange servers

Before you can back up your databases using SnapManager, you need to run the SnapManager Configuration wizard for each Exchange server. You use the Configuration wizard to migrate databases to NetApp storage and to configure SnapManager for your Exchange servers.

About this task

Attention: SnapManager takes Exchange databases offline when it migrates them.

You use the SnapManager Configuration wizard to select a backup set verification server, migrate databases and logs to NetApp storage, map databases and logs to their respective SnapInfo directories, and configure automatic event notification.

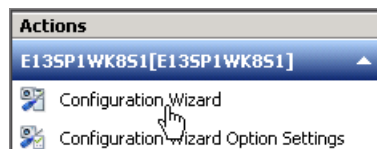
When migrating databases, SnapManager ensures that the files are placed in locations that meet SnapManager configuration requirements. If you use a separate tool to migrate databases or logs, run the Configuration wizard to ensure that the files are in correct locations. Incorrectly located files can impair SnapManager operations.

Even if you create new databases directly on NetApp storage, you need to run the Configuration wizard to create a mapping between those databases and the SnapInfo directory.

If you have a Database Availability Group (DAG), run the Configuration wizard on each DAG member and then on the DAG itself.

Steps

1. If the **Configuration** wizard is not open, in the **Actions** menu, click **Configuration Wizard**.



2. On the **Start** page, click **Next**.

The Start page includes an option to use a *control file*. A control file contains configuration details about an Exchange server. You might use this option at another time to export and then import a configuration. For information about using control files, see the [SnapManager 7.2 for Microsoft Exchange Server Administration Guide](#).

3. In the **Verification Settings** page, define how SnapManager should verify backup copies:

For this field...	Do this...
Verification Server	For optimal performance, choose a remote verification server, which offloads work from the Exchange production server.
Access LUN in a Snapshot	Keep the default option for mounting Snapshot copies to an empty NTFS directory. SnapManager mounts the Snapshot copy to the verification server when it verifies the backup. An empty NTFS directory is typically better than assigning drive letters because the verification server can run out of drive letters if there are more backup copies than available drive letters.

4. On the **Exchange Server to Configure** page, click **Next**.
5. On the **Migrate storage to LUNs** page, assign your databases to LUNs and then view the results of your selections:

a. In the **Storage Group/Database** pane, select a database:

Storage Group/Database	Disk
Mailbox Database 0...	Local[SG ED]
E13SP1wK8S1_A...	Local[SG ED]

b. In the **Available Disks** pane, select a LUN:

Available Disks	
LUN G	
LUN I	
LUN J	
LUN K	

c. Click the  button.

d. Repeat substeps a to c for each database.

e. In the **Database Location Results** pane, review the results of your selections:

Database Location Results		
Storage Group/Database	From	To
E13SP1wK8S1_AU...	LUN F	LUN F
E13SP1wK8S1_AU...	LUN H	LUN H
E13SP1wK8S1_AU...	Local[SG...	K

Tip: To change your selections, click **Undo All** or select a database and click **Reconfigure**.

6. On the next **Migrate storage to LUNs** page, specify the LUNs on which you want to place transaction logs for each database.
7. On the **Configure SnapInfo Directory** page, specify the LUNs on which you want to place SnapInfo directories for each database.
8. On the **Configure Dataset** page, click **Next**.
 Datasets are used for SnapVault integration with Data ONTAP operating in 7-Mode only.
9. On the **iSCSI Dependency** page, choose whether to set the iSCSI service as a dependency and click **Next**:
 - If you use iSCSI, you should keep the option selected.
 - If you do not use iSCSI, clear the option.

Setting the iSCSI service as a dependency for all Exchange Server services helps protect Exchange data if there is a problem with iSCSI.

10. On the **Auto Support Settings** page, configure settings for email notifications, event logging, and AutoSupport notifications.

Most of the fields on this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Send e-mail notification	Enables email notifications to the specified address about the success or failure of SnapManager operations. If you select this field, click Advanced to tune the notification settings—for example, to receive notifications only when operations fail.

Field	Description
Log SnapManager events to storage system syslog	Posts SnapManager events to the storage system's event log, if AutoSupport is enabled on the storage system. Technical support can use this information to troubleshoot issues.
Send AutoSupport notification	Enables email notifications to technical support about SnapManager events or storage system problems that might occur, if AutoSupport is enabled on the storage system.
On failure only	Limits the SnapManager events that are posted to the storage system event log and sent through AutoSupport to failure events only.

- On the **Monitoring and Reporting Settings** page, choose whether you want to receive recurring email notifications that contain the status of backup and verification operations.

To receive email notifications, you must have enabled email notifications on the previous page.

Important: Set the report to run after your backup schedule. If the report runs at the same time as the backups, the report might incorrectly state that the backups failed.

- On the **Finish** page, review the settings and click **Finish**.

SnapManager migrates the databases and updates your SnapManager configuration. You can view details of the operation in the Configuration Report.

After you finish

Rerun the Configuration wizard at any time to review or make changes to your database configurations.

If you add or move databases, you should run the Configuration wizard to ensure that the databases are stored in valid locations and to create a mapping between those databases and their respective SnapInfo directories.

Preparing storage systems for SnapMirror and SnapVault replication

You can use SnapManager with ONTAP SnapMirror technology to create mirror copies of backup sets on another volume, and with ONTAP SnapVault technology to perform disk-to-disk backup replication for standards compliance and other governance-related purposes. Before you perform these tasks, you must configure a *data-protection relationship* between the source and destination volumes and *initialize* the relationship.

A data protection relationship replicates data on primary storage (the source volume) to secondary storage (the destination volume). When you initialize the relationship, ONTAP transfers the data blocks referenced on the source volume to the destination volume.

Note: If you are using SnapDrive 7.1 for Windows, you cannot configure both a SnapMirror relationship and a SnapVault relationship on the same ONTAP source volume. You must configure these relationships on different source volumes. This limitation does not exist starting with SnapDrive 7.1.1 for Windows.

SnapManager does not support cascade relationships between SnapMirror and SnapVault volumes (**Primary > Mirror > Vault**). Use fanout relationships only (**Primary > Mirror, Primary > Vault**).

Related tasks

[Understanding the differences between SnapMirror and SnapVault](#) on page 23

[Preparing storage systems for SnapMirror replication](#) on page 24

[Preparing storage systems for SnapVault replication](#) on page 25

Understanding the differences between SnapMirror and SnapVault

SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. SnapVault is disk-to-disk backup replication technology, designed for standards compliance and other governance-related purposes.

These objectives account for the different balance each technology strikes between the goals of backup currency and backup retention:

- SnapMirror stores *only* the Snapshot copies that reside in primary storage, because, in the event of a disaster, you need to be able to fail over to the most recent version of primary data you know to be good.
Your organization, for example, might mirror hourly copies of production data over a ten-day span. As the failover use case implies, the equipment on the secondary system must be equivalent or nearly equivalent to the equipment on the primary system to serve data efficiently from mirrored storage.
- SnapVault, in contrast, stores Snapshot copies *whether or not* they currently reside in primary storage, because, in the event of an audit, access to historical data is likely to be as important as access to current data.
You might want to keep monthly Snapshot copies of your data over a 20-year span, for example, to comply with government accounting regulations for your business. Because there is no requirement to serve data from secondary storage, you can use slower, less expensive disks on the vault system.

The different weights that SnapMirror and SnapVault give to backup currency and backup retention ultimately derive from the limit of 255 Snapshot copies for each volume. While SnapMirror retains the most recent copies, SnapVault retains the copies made over the longest period of time.

Preparing storage systems for SnapMirror replication

Before you can use SnapManager to mirror Snapshot copies, you need to configure a *data-protection relationship* between the source and destination volumes, then initialize the relationship. Upon initialization, SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks that it references to the destination volume. It also transfers any other, less recent Snapshot copies on the source volume to the destination volume.

Before you begin

- You must have created the source and destination volumes in peered clusters with peered storage virtual machines (SVMs).

[Cluster and SVM Peering Express Guide](#)

- You must be a cluster administrator.
- For Snapshot copy verification on the destination volume, the source and destination storage virtual machines (SVMs) must have a management LIF as well as a data LIF.

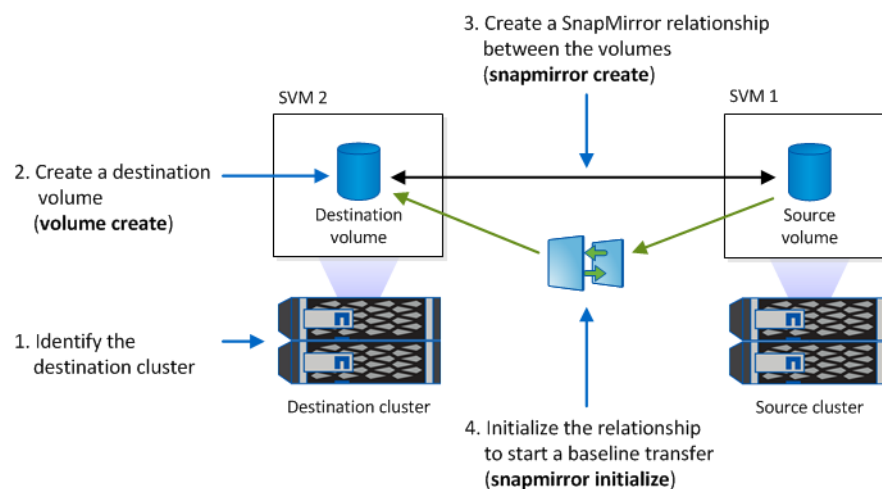
The management LIF must have the same DNS name as the SVM. Set the management LIF role to **data**, the protocol to **none**, and the firewall policy to **mgmt**.

About this task

You can use the ONTAP command-line interface (CLI) or ONTAP System Manager to create a SnapMirror relationship. The following procedure documents CLI usage.

Important: If you are storing database files and transaction logs on different volumes, you must create relationships between the source and destination volumes for the database files and between the source and destination volumes for the transaction logs.

The following illustration shows the procedure for initializing a SnapMirror relationship:



Steps

1. Identify the destination cluster.

2. On the destination cluster, use the `volume create` command with the `-type DP` option to create a SnapMirror destination volume that is either the same or greater in size than the source volume.

Important: The language setting of the destination volume must match the language setting of the source volume.

Example

The following command creates a 2 GB destination volume named `dstvolB` in SVM2 on the aggregate `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr -type DP
-size 2GB
```

3. On the destination SVM, use the `snapmirror create` command with the `-type DP` parameter to create a SnapMirror relationship.

The `DP` type defines the relationship as a SnapMirror relationship.

Example

The following command creates a SnapMirror relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2, and assigns the default SnapMirror policy `DPDefault`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path SVM2:dstvolB
-type DP
```

Note: Do not define a mirror schedule for the SnapMirror relationship. SnapManager does that for you when you create a backup schedule.

If you do not want to use the default SnapMirror policy, you can invoke the `snapmirror policy create` command to define a SnapMirror policy.

4. Use the `snapmirror initialize` command to initialize the relationship.

The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it references to the destination volume. It also transfers any other Snapshot copies on the source volume to the destination volume.

Example

The following command initializes the relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Preparing storage systems for SnapVault replication

Before you can use SnapManager to perform disk-to-disk backup replication, you need to configure a *data-protection relationship* between the source and destination volumes, then initialize the relationship. On initialization, SnapVault makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it references to the destination volume.

Before you begin

- You must have created the source and destination volumes in peered clusters with peered storage virtual machines (SVMs).

Cluster and SVM Peering Express Guide

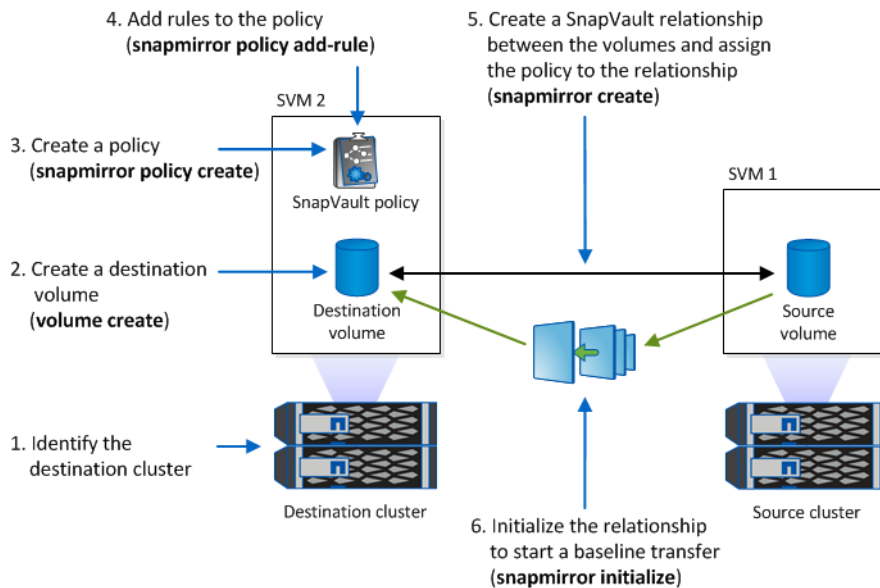
- You must be a cluster administrator.

About this task

You can use the ONTAP command-line interface (CLI) or ONTAP System Manager to create SnapVault relationships. The following procedure documents CLI usage.

Important: If you are storing database files and transaction logs on different volumes, you must create relationships between the source and destination volumes for the database files and between the source and destination volumes for the transaction logs.

The following illustration shows the procedure for initializing a SnapVault relationship:

**Steps**

- Identify the destination cluster.
- On the destination cluster, use the `volume create` command with the `-type DP` option to create a SnapVault destination volume that is the same size as or larger than the source volume.

Important: The language setting of the destination volume must match the language setting of the source volume.

Example

The following command creates a 2 GB destination volume named `dstvolB` in SVM2 on the aggregate `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr -type DP
-size 2GB
```

- On the destination SVM, use the `snapmirror policy create` command to create a SnapVault policy.

Example

The following command creates the SVM-wide policy `SVM1-vault`:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-vault
```

Note: Do not define a cron schedule or Snapshot copy policy for the SnapVault relationship. SnapManager does that for you when you create a backup schedule.

4. Use the `snapmirror policy add-rule` command to add rules to the policy that define the following Snapshot copy labels and the retention policy for each label:
 - Daily
 - Weekly
 - Monthly
 - Hourly
 - Unlimited

Important: The labels are case-sensitive.

These are fixed labels for options displayed when you perform a backup. You select one of these options when you archive the backup. You must execute this command once for each of the rules you are adding.

Example

The following command adds a rule to the SVM1-vault policy that defines the “Daily” label and specifies that 30 Snapshot copies matching the label should be kept in the vault:

```
SVM2::> snapmirror policy add-rule -vserver SVM2 -policy SVM1-vault
-snapmirror-label Daily -keep 30
```

5. Use the `snapmirror create` command with the `-type XDP` parameter and the `-policy` parameter to create a SnapVault relationship and assign a vault policy.

The **XDP** type defines the relationship as a SnapVault relationship.

Example

The following command creates a SnapVault relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2, and assigns the policy `SVM1-vault`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path SVM2:dstvolB
-type XDP -policy SVM1-vault
```

6. Use the `snapmirror initialize` command to initialize the relationship.

The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it references to the destination volume.

Example

The following command initializes the relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Backing up and verifying your databases

You should back up your databases as soon as they are available in NetApp storage. You can then verify the initial backups and schedule recurring backups and recurring backup verifications.

Related tasks

- [SnapManager backup overview](#) on page 28
- [Defining a backup strategy](#) on page 28
- [Backing up your databases for the first time](#) on page 31
- [Verifying the initial backup set](#) on page 33
- [Scheduling recurring backups](#) on page 33
- [Scheduling frequent recovery point backups](#) on page 34
- [Scheduling recurring backup set verifications](#) on page 35

SnapManager backup overview

SnapManager uses NetApp Snapshot technology to create online, read-only copies of databases. It uses an Exchange Server tool to verify the integrity of the backups.

SnapManager backs up a database by creating Snapshot copies of the volumes in which the following reside:

- Database data files
- SnapInfo directories and transaction logs

Together these Snapshot copies comprise a *backup set*. SnapManager uses a backup set to restore a database.

After SnapManager backs up your databases, it can perform an integrity verification of the backup sets. SnapManager uses the Exchange System Management Tools to check the database and transaction log files for physical and logical corruption. Verification ensures that you can use backup sets to restore databases as needed.

Note: Database verification is disabled by default if you have a Database Availability Group (DAG). Verification is not required for DAG databases that have at least two copies, each of which has a viable backup. For more information, see [NetApp KB Article 3013600: Does verification in SME need to occur in an Exchange 2010 DAG deployment?](#)

Important: SnapManager cannot restore databases from Snapshot copies created by Data ONTAP or SnapDrive. You should perform backups using SnapManager only.

Defining a backup strategy

Defining a backup strategy before you create your backup jobs helps ensure that you have the backups that you need to successfully restore your databases. Your Service Level Agreement (SLA) and Recovery Point Objective (RPO) largely determine your backup strategy.

Note: For SnapManager best practices, see [NetApp Technical Report 4221: Microsoft Exchange Server 2013 and SnapManager for Exchange Best Practices Guide for Clustered Data ONTAP](#).

What type of SnapManager backup do you need?

SnapManager supports two types of backups:

Backup type	Description
Database backup	<p>You can choose from two database backups:</p> <ul style="list-style-type: none"> • Full backup Backs up database files and truncated transaction logs. Exchange Server truncates transaction logs by removing entries already committed to the database. This is the most common backup type. • Copy backup Backs up database files and transaction logs that have not been truncated. Use this backup type when you are backing up your databases with another backup application. Keeping transaction logs intact ensures that any backup application can restore the databases. For information about the remote additional copy backup feature, see the SnapManager 7.2 for Microsoft Exchange Server Administration Guide.
Frequent recovery point backup (FRP)	<p>Backs up truncated transaction logs, copying only transactions committed after the most recent full backup or FRP backup.</p> <p>If you schedule frequent recovery point backups to work with database backups, SnapManager can restore databases to a specific recovery point more quickly. For example, you might schedule database backups at the start and end of the day and frequent recovery point backups every hour.</p> <p>SnapManager does not verify transaction logs when it creates frequent recovery point backups. SnapManager verifies the backups when it verifies the backup sets created from database backups.</p>

When should you back up your databases?

The most critical factor for determining a database backup schedule is the rate of change for the database. You might back up a heavily used database every hour, while you might back up a rarely used database once a day. Other factors include the importance of the database to your organization, your Service Level Agreement (SLA), and your Recover Point Objective (RPO).

Even for a heavily used database, there is no requirement to run a full backup more than once or twice a day. Regular transaction log backups are usually sufficient to ensure that you have the backups you need.

Tip: The more often you back up your databases, the fewer transaction logs SnapManager has to play forward at restore time, which can result in faster restore operations.

Important: SnapManager can perform one operation at a time. Do not schedule overlapping SnapManager operations.

When should you verify backup copies?

Although SnapManager can verify backup sets immediately after it creates them, doing so can significantly increase the time required to complete the backup job. It is almost always best to schedule verification in a separate job at a later time. For example, if you back up a database at 5:00 p.m. every day, you might schedule verification to occur an hour later at 6:00 p.m.

For the same reason, it is usually not necessary to run backup set verification every time you perform a backup. Performing verification at regular but less frequent intervals is usually sufficient to ensure the integrity of the backup. A single verification job can verify multiple backup sets at the same time.

Note: Verification is not required for DAG databases that have at least two copies, each of which has a viable backup. For more information, see [NetApp KB Article 3013600: Does verification in SME need to occur in an Exchange 2010 DAG deployment?](#)

Important: SnapManager can perform one operation at a time. Do not schedule overlapping SnapManager operations.



How many backup jobs do you need?

You can back up your databases using one backup job or several. The number of backup jobs that you choose typically mirrors the number of volumes on which you placed your databases. For example, if you placed a group of small databases on one volume and a large database on another volume, you might create one backup job for the small databases and one backup job for the large database.

Other factors that determine the number of backup jobs that you need include the size of the database, its rate of change, and your Service Level Agreement (SLA).

Which backup naming convention do you want to use?

A backup naming convention adds a string to Snapshot copy names. The string helps you identify when the copies were created. There are two naming conventions:



Naming convention	Description
Unique	Adds a time stamp to all Snapshot copy names. This is the default option. Example:  exchsnap__E13SP1WK8S1_07-02-2014_10.45.13
Generic	Adds the string “recent” to the name of the most recent Snapshot copy. All other Snapshot copies include a time stamp. Example:  exchsnap__E13SP1WK8S1__recent

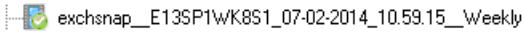
The selected naming convention applies to all backups. You should use the unique naming convention unless you have a script that requires the constant string “recent”.

You can change the naming convention in the **Backup Settings** dialog box.

Which backup management group do you want to assign to the backup job?

You select a backup management group to apply a labeling convention to Snapshot copies. When you back up a database, you can choose from three management groups:

Management group	Description
Standard	Does not include the name of the management group in Snapshot copy names. Example:  exchsnap__E13SP1WK8S1_07-02-2014_10.45.13
Daily	Adds “Daily” to Snapshot copy names. Example:  exchsnap__E13SP1WK8S1_07-02-2014_10.53.59__Daily

Management group	Description
Weekly	Adds “Weekly” to Snapshot copy names. Example: 

For example, if you schedule daily and weekly backups, you should assign the backups to the Daily and Weekly management groups, respectively.

Note: Management groups do not enforce a backup schedule.

How long do you want to retain backup copies on the source storage system and the SnapMirror destination?

You can choose either the number of days you want to retain backup copies, or specify the number of backup copies you want to retain, up to 255. For example, your organization might require that you retain 10 days worth of backup copies.

If you set up SnapMirror replication, the retention policy is mirrored on the destination volume.

Note: For long-term retention of backup copies, you should use SnapVault.

How long do you want to retain transaction log backups on the source storage system?

SnapManager needs transaction log backups to perform *up-to-the-minute restore operations*, which restore your database to a time between two full backups. For example, if SnapManager took a full backup at 8:00 a.m. and another full backup at 5:00 p.m, it could use the latest transaction log backup to restore the database to any time between 8:00 a.m. and 5:00 p.m. If transaction logs are not available, SnapManager can perform *point-in-time restore operations* only, which restore a database to the time that SnapManager completed a full backup.

Typically, you require up-to-the-minute restores for only a day or two, which means you would retain transaction log backups for one or two days.

Do you want to verify backup copies using the source volume or destination volume?

If you use SnapMirror or SnapVault, you can verify backup copies using the Snapshot copy on the SnapMirror or SnapVault destination volume, rather than the Snapshot copy on the primary storage system. Verification using a destination volume reduces load on the primary storage system.

If you need to create backups using another tool, what backup type should you use?

If you need to create backups using another backup tool, create copy or differential backups only with that tool. Normal (full) and incremental backups truncate transaction logs, effectively disabling SnapManager up-to-the-minute restores.

Backing up your databases for the first time

After you migrate your databases to NetApp storage, you should back them up immediately. You can schedule recurring backups after the initial backup and verification.

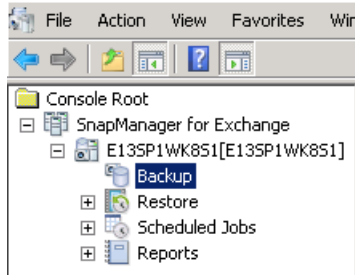
About this task

These steps show you how to quickly back up your databases using the Backup and Verify option. You can use the Backup wizard if you prefer.

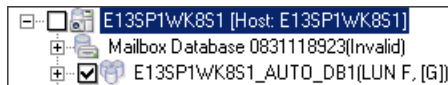
If you have a Database Availability Group (DAG), you can back up all databases in the group by running the backup job from the DAG. You cannot back up at the DAG level if nodes in the DAG use non-NetApp storage. You must back up the databases from each DAG member instead.

Steps

1. In the **Console Root** tree, expand the server on which the databases reside and click **Backup**.



2. In the **Backup** pane, select the databases that you want to backup.



3. In the **Actions** pane, click **Backup and Verify**.



4. In the **Backup** dialog box, keep **Create backup** selected and define the properties for the backup job:

For this field...	Do this...
Delete backup	Specify a retention policy for backup copies on the source storage system by defining the number of backup copies to retain or the number of days to retain backup copies.
Up-to-minute Restore options	Click this field and then specify a retention policy for transaction logs.
Verify backed up databases and transaction logs	Clear this field because it is best to verify databases in a separate operation.
Backup management group	Select a management group.
Run command after operation	If you want to run a command after the backup operation, select this field. You specify the command after you click Backup .
Backup archiving options	If you set up a SnapVault destination volume, select the option to archive the backup copy to the destination volume.
SnapMirror options	If you set up a SnapMirror destination volume, select the option to replicate the backup copy to the destination volume.
Advanced Options	If you back up your databases using another backup application, click this field, then click Backup Type , and finally select Copy backup . Keep the default selections for other fields in the advanced options.

5. Click **Backup**.
6. If you chose to run a command after the operation, specify where to run the command, the path to the program or script, the SnapManager variables to execute, and the command arguments, and then click **OK**.

7. In the Backup Status dialog box, click **Start Now**.

You can view details of the operation in the Backup Task List and Backup Report tabs.

Verifying the initial backup set

You should verify an initial backup set to confirm the integrity of the databases.

Steps

1. In the **Backup** pane, select the databases that you want to include in the backup verification schedule.
2. In the **Actions** pane, click **Backup and Verify**.
3. In the **Backup** dialog box, select **Verify backup sets** and then define the properties for the backup verification:

For this field...	Do this...
Select the number of recent unverified backups to be verified	Keep the default. You should have only one backup set at this point.
Backup management group	Select a management group.
Run command after operation	If you want to run a command after the backup operation, enable the field. You specify the command after you click Verify .
Backup archiving options	If you archived the backup set to a SnapVault destination volume and you want to verify the backup set on the destination storage system to reduce load on the primary storage system, click Verify on previously archived backup .
SnapMirror options	If you replicated the backup set to a SnapMirror destination volume and you want to verify the backup set on the destination storage system to reduce load on the primary storage system, click Verify on available SnapMirror destination volumes .

4. Click **Verify**.
5. If you chose to run a command after the operation, specify where to run the command, the path to the program or script, the SnapManager variables to execute, and the command arguments, and then click **OK**.
6. In the Backup Status dialog box, click **Start Now**.

You can view details of the operation in the Backup Task List and Backup Report tabs.

Scheduling recurring backups

You can schedule recurring backup jobs using Windows Scheduled Tasks.

Steps

1. In the **Backup** pane, select the databases that you want to include in the backup schedule.
2. In the **Actions** pane, click **Backup and Verify**.
3. In the **Backup** dialog box, keep **Create backup** selected and define the properties for the backup schedule, as described in [Backing up your databases for the first time](#) on page 31.

4. Click **Schedule**.
5. In the **Schedule** dialog box, enter a job name, enter your credentials, and click **OK**.
6. Create the schedule using Windows Scheduled Tasks:
 - a. Click **Schedule**.
 - b. Specify the schedule.
 - c. Click **OK**.
 - d. Click **Yes** to save the job.

After you finish

You can view details about the backup job in the SnapManager Scheduled Jobs pane.

Scheduling frequent recovery point backups

Frequent recovery point backups help you preserve transaction logs. You should schedule transaction log backups alongside full database backups at a frequency that allow you to meet your Recovery Point Objective (RPO).

Steps

1. In the **Console Root** tree, select the server on which the databases reside.
2. In the **Actions** pane, click **Frequent Recovery Point Backup**.
3. In the **Frequent Recovery Point Backup** dialog box, define the properties for the transaction log backup schedule:

For this field...	Do this...
Selected for backup	Select the databases that you want to include in the backup schedule.
Backup frequency	Specify how often you want to back up the transaction logs.
Run command after operation	If you want to run a command after the backup operation, select this field. You specify the command after you click Create Job .
Update SnapMirror after operation	If you set up a SnapMirror destination volume, select this field to replicate the backup copy to the destination volume.

4. Click **Create Job**.
5. Create the schedule using **Windows Scheduled Tasks**:
 - a. Click **Schedule**.
 - b. Specify the schedule.
 - c. Click **OK**.
 - d. Click **Yes** to save the job.

Scheduling recurring backup set verifications

You can schedule recurring backup set-verification jobs using Windows Scheduled Tasks.

Steps

1. In the **Backup** pane, select the databases that you want to include in the backup verification schedule.
2. In the **Actions** pane, click **Backup and Verify**.
3. In the **Backup** dialog box, select **Verify backup sets** and define the properties for the backup verification schedule as described in [Verifying the initial backup set](#) on page 33.

You might need to modify the **Number of recent unverified backups to be verified** field, depending on the number of backups SnapManager will take between scheduled verifications.

4. Click **Schedule**.
5. In the **Schedule** dialog box, enter a job name, enter your credentials, and click **OK**.
6. Create the schedule using Windows Scheduled Tasks:
 - a. Click **Schedule**.
 - b. Specify the schedule.
 - c. Click **OK**.
 - d. Click **Yes** to save the job.

After you finish

You can view details about the verification job in the SnapManager Scheduled Jobs pane.

Where to go next

After you have configured backups in SnapManager, you can perform full or partial restores as necessary. You can also explore other important SnapManager features, such as reports, control files, and PowerShell cmdlets.

You can find more information about these features, as well as release-specific information for SnapManager, in the following documentation, available on the NetApp Support Site.

- [*SnapManager 7.2 for Microsoft Exchange Server Administration Guide*](#)
Describes how to administer SnapManager after deployment is complete. Topics include how to restore the database, how to import configuration information from a control file, how to use the SnapManager PowerShell cmdlets, and how to upgrade and uninstall the product.
- [*SnapManager 7.2.1 for Microsoft Exchange Server Release Notes*](#)
Describes new features, important cautions, known problems, and limitations for the SnapManager 7.x product.
- [*Single Mailbox Recovery 7.1 Administration Guide*](#)
Describes how to use the Single Mailbox Recovery product.
- [*Cluster and SVM Peering Express Guide*](#)
Describes how to quickly configure peer relationships between clusters and SVMs.
- [*ONTAP 9 Volume Disaster Recovery Preparation Express Guide*](#)
Describes how to prepare storage system for SnapMirror replication.
- [*ONTAP 9 Volume Backup Using SnapVault Express Guide*](#)
Describes how to prepare storage system for SnapVault replication.
- [*NetApp Technical Report 4221: Microsoft Exchange Server 2013 and SnapManager for Exchange Best Practices Guide for Clustered Data ONTAP*](#)
Describes SnapManager for Microsoft Exchange Server best practices.

Copyright

Copyright © 2020 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

[*doccomments@netapp.com*](mailto:doccomments@netapp.com)

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

- additional information
 - about SnapManager features [36](#)
- administration server
 - Windows host requirements [12](#)
- AutoSupport
 - configuring [20](#)

B

- backing up databases
 - for the first time [31](#)
 - using a schedule [33](#)
- backup sets
 - verifying the initial set [33](#)
 - verifying with a schedule [35](#)
- backup types
 - overview of [28](#)
- backups
 - using SnapMirror and SnapVault replication [23](#)
- base configuration
 - Windows host requirements [12](#)
- benefits and features
 - overview of [4](#)
- best practices [9](#)

C

- comments
 - how to send feedback about documentation [39](#)
- configuration
 - workflow [6](#)

D

- Database Availability Group
 - installing SnapManager on [16](#)
- Database Availability Groups
 - connecting to [19](#)
- databases
 - backing up for the first time [31](#)
 - backing up with a schedule [33](#)
 - migrating to NetApp storage [20](#)
 - name requirements [19](#)
 - overview of backing up [28](#)
 - preparing for SnapMirror replication [24](#)
 - preparing storage systems for SnapVault replication [25](#)
 - prerequisites for migrating [19](#)
 - strategy for backing up [28](#)
 - verifying the initial backup set [33](#)
 - verifying with a schedule [35](#)
- deployment
 - preparing, SnapManager [7](#)
- documentation
 - how to receive automatic notification of changes to [39](#)

- how to send feedback about [39](#)

E

- email notifications
 - configuring [20](#)
- Exchange Servers
 - connecting SnapManager to [19](#)

F

- features
 - where to find additional information about SnapManager [36](#)
- features and benefits
 - overview of [4](#)
- feedback
 - how to send comments about documentation [39](#)

I

- IMT
 - using to verify support for system configurations [10](#)
 - verifying your configuration [7](#)
- information
 - how to send feedback about improving documentation [39](#)
- installing SnapManager
 - interactively [16](#)
 - on Database Availability Group [16](#)
 - silently [17](#)
 - workflow [6](#)
- Interoperability Matrix Tool
 - See* IMT

M

- management groups
 - overview of [28](#)
- migrating
 - database files [20](#)
 - prerequisites for [19](#)
 - transaction logs [20](#)

N

- naming conventions
 - overview of [28](#)
- NetApp Interoperability Matrix Tool
 - See* IMT

P

- per-server licensing
 - SnapManager for Microsoft Exchange Server [9](#)
- per-storage system licensing
 - SnapManager for Microsoft Exchange Server [9](#)

- preparations
 - for deployment, SnapManager 7
- product overview
 - features and benefits 4

R

- Recovery Point Objective
 - meeting 34
- replication
 - considerations for preparing storage systems for SnapMirror and SnapVault 23
 - preparing storage systems for SnapMirror 24
 - preparing storage systems for SnapVault 25
- requirements
 - service account 13

S

- service accounts
 - requirements 13
- SnapInfo directory
 - mapping to data files and logs 20
- SnapManager
 - supported storage types 11
 - where to find additional information about features 36
- SnapManager for Microsoft Exchange Server
 - administration server 9, 12
 - archiving Snapshot copies 25
 - backup overview 28
 - backup strategy 28
 - base configuration 9, 12
 - connecting to Exchange Servers 19
 - deployment workflow 6
 - features and benefits 4
 - installing
 - interactively 16
 - silently 17
 - licensing 9
 - mirroring Snapshot copies 24
 - storage layout requirements 7
 - verification server 9, 12
 - Windows Firewall requirements 12
 - Windows host requirements 12
- SnapMirror
 - considerations for preparing storage systems for replication 23

- differences from SnapVault 23
 - preparing storage systems for replication 24
- Snapshot copies
 - preparing for SnapVault replication 25
 - preparing storage systems for SnapMirror replication 24
- SnapVault
 - considerations for preparing storage systems for replication 23
 - differences from SnapMirror 23
 - preparing storage systems for replication 25
- storage layout requirements
 - for SnapManager for Microsoft Exchange Server 7
- storage systems
 - considerations for preparing for SnapMirror and SnapVault replication 23
- storage types
 - supported by SnapManager 11
- suggestions
 - how to send feedback about documentation 39
- support
 - storage types 11
 - verifying SnapManager support for system configurations 10
- system configurations
 - verifying SnapManager support for 10
- systems
 - considerations for preparing for SnapMirror and SnapVault replication 23

T

- transaction log backups
 - using a schedule 34
- transaction logs
 - backing up with a schedule 34
- Twitter
 - how to receive automatic notification of documentation changes 39

V

- verification server
 - selecting 20
 - Windows host requirements 12