Installation and Setup for UNIX for 7-mode

SnapManager for SAP

NetApp
November 04, 2025

Table of Contents

Installation and Setup for UNIX for 7-mode . . . 1
- Product overview . . . 1
  - SnapManager highlights . . . 1
  - SnapManager architecture . . . 2
- Deployment workflow . . . 3
- Prepare for deployment . . . 4
  - SnapManager licensing . . . 4
  - Supported configurations . . . 5
  - Supported storage types . . . 6
  - UNIX host requirements . . . 6
- Configure databases . . . 7
- Install SnapManager . . . 7
- Set up SnapManager . . . 7
- Preparing storage systems for SnapMirror and SnapVault replication . . . 7
  - Understanding the differences between SnapMirror and SnapVault . . . 7
- Backing up and verifying your databases . . . 8
  - SnapManager backup overview . . . 8
  - Defining a backup strategy . . . 8
- Upgrading SnapManager . . . 10
  - Preparing to upgrade SnapManager . . . 10
  - Post-upgrade tasks . . . 11
  - Upgrading SnapManager hosts by using rolling upgrade . . . 11
- Where to go next . . . 16

Installation and Setup for UNIX for 7-mode

Product overview

SnapManager for SAP automates and simplifies the complex, manual, and time-consuming processes associated with the backup, recovery, and cloning of databases. You can use SnapManager with ONTAP SnapMirror technology to create copies of backups on another volume and with ONTAP SnapVault technology to archive backups efficiently to disk.

SnapManager provides the tools required, such as OnCommand Unified Manager and integration with SAP's BR* Tools, to perform policy-driven data management, schedule and create regular database backups, and restore data from these backups in the event of data loss or disaster.

SnapManager also integrates with native Oracle technologies, such as Oracle Real Application Clusters (Oracle RAC) and Oracle Recovery Manager (RMAN) to preserve backup information. These backups can be used later in block-level restore or tablespace point-in-time recovery operations.

SnapManager highlights

SnapManager features seamless integration with databases on the UNIX host and with Snapshot, SnapRestore, and FlexClone technologies on the back end. It offers an easy-to-use user interface (UI) as well as command-line interface (CLI) for administrative functions.

SnapManager enables you to perform the following database operations and manage data efficiently:

- Creating space-efficient backups on primary or secondary storage

  SnapManager enables you to back up the data files and archive log files separately.

- Scheduling backups
- Restoring full or partial databases by using a file-based or volume-based restore operation
- Recovering databases by discovering, mounting, and applying archive log files from backups
- Pruning archive log files from archive log destinations when creating backups of only the archive logs
- Retaining a minimum number of archive log backups automatically by retaining only the backups that contain unique archive log files
- Tracking operation details and generating reports
- Verifying backups to ensure that backups are in a valid block format and that none of the backed-up files are corrupted
- Maintaining a history of operations performed on the database profile

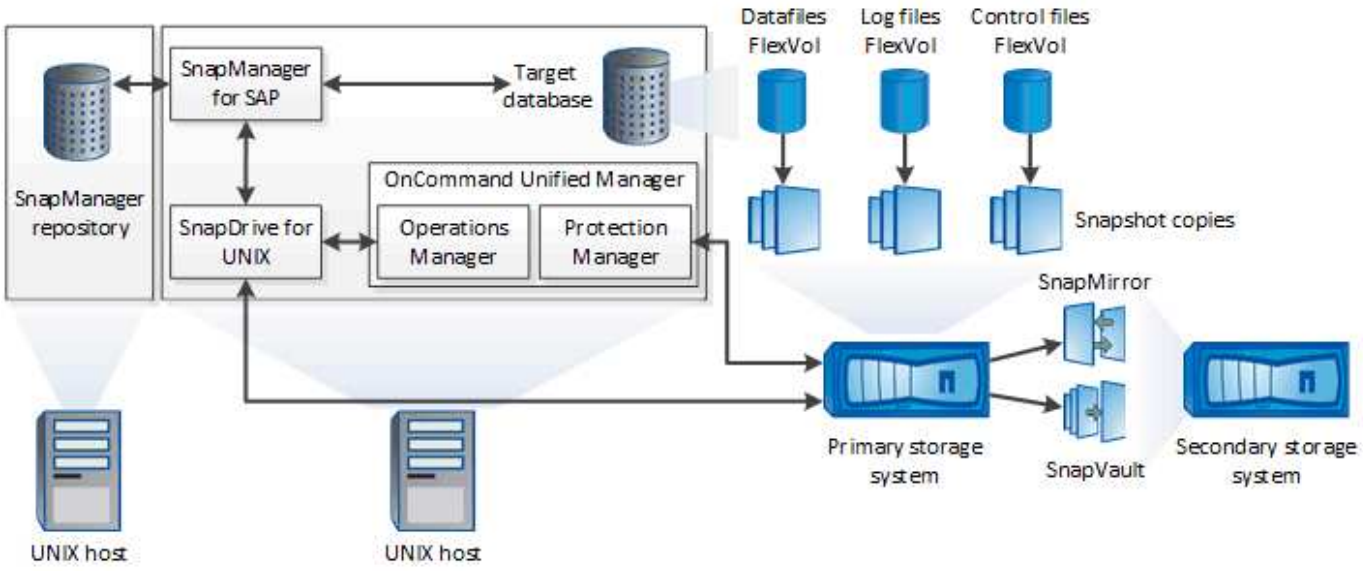
  A profile contains information about the database to be managed by SnapManager.

- Protecting backups on the secondary and tertiary storage systems.
- Creating space-efficient clones of backups on primary or secondary storage

  SnapManager enables you to split a clone of a database.

SnapManager architecture

SnapManager for SAP includes components that work together to provide a comprehensive and powerful backup, restore, recovery, and cloning solution for Oracle databases.



SnapDrive for UNIX

SnapManager requires SnapDrive to establish connection with the storage system. You must install SnapDrive for UNIX on every target database host before installing SnapManager.

SnapManager for SAP

You must install SnapManager for SAP on every target database host.

You can either use the command-line interface (CLI) or UI from the database host where SnapManager for SAP is installed. You can also use the SnapManager UI remotely by using a web browser from any system running on an operating system supported by SnapManager.

The supported JRE version is 1.8.

Target database

The target database is an Oracle database that you want to manage using SnapManager by performing backup, restore, recovery, and clone operations.

The target database can be a standalone, Real Application Clusters (RAC), or reside on Oracle Automatic Storage Management (ASM) volumes. For details about the supported Oracle database versions, configurations, operating systems, and protocols, see the NetApp Interoperability Matrix Tool.

SnapManager repository

The SnapManager repository resides in an Oracle database and stores metadata about profiles, backups, restore, recovery, and clone. A single repository can contain information about operations performed on multiple database profiles.

The SnapManager repository cannot reside in the target database. The SnapManager repository database and the target database must be online before performing SnapManager operations.

OnCommand Unified Manager Core Package

OnCommand Unified Manager core package integrates the capabilities of Operations Manager, Protection Manager, and Provisioning Manager. It centralizes provisioning, cloning, backup and recovery, and disaster recovery (DR) policies. Integrating all of these capabilities makes it possible to perform many management functions from a single tool.

Operations Manager

Operations Manager is the web-based user interface (UI) of the OnCommand Unified Manager core package. It is used for day-to-day storage monitoring, issue alerts, and reporting on storage and storage system infrastructure. SnapManager integration leverages the RBAC capabilities of Operations Manager.

Protection Manager

Protection Manager gives administrators an easy-to-use management console for quick configuration and control of all SnapMirror and SnapVault operations. The application allows administrators to apply consistent data protection policies, automate complex data protection processes, and pool backup and replication resources for higher utilization.

The interface for Protection Manager is the NetApp Management Console, the client platform for NetApp management software applications. TheNetApp Management Console runs on a Windows or Linux system that is different from the server on which the OnCommand server is installed. It enables storage, application, and server administrators to perform daily tasks without having to switch between different UIs. The applications that run in the NetApp Management Console are Protection Manager, Provisioning Manager, and Performance Advisor.

Primary storage system

SnapManager backs up the target databases on the primary NetApp storage system.

Secondary storage system

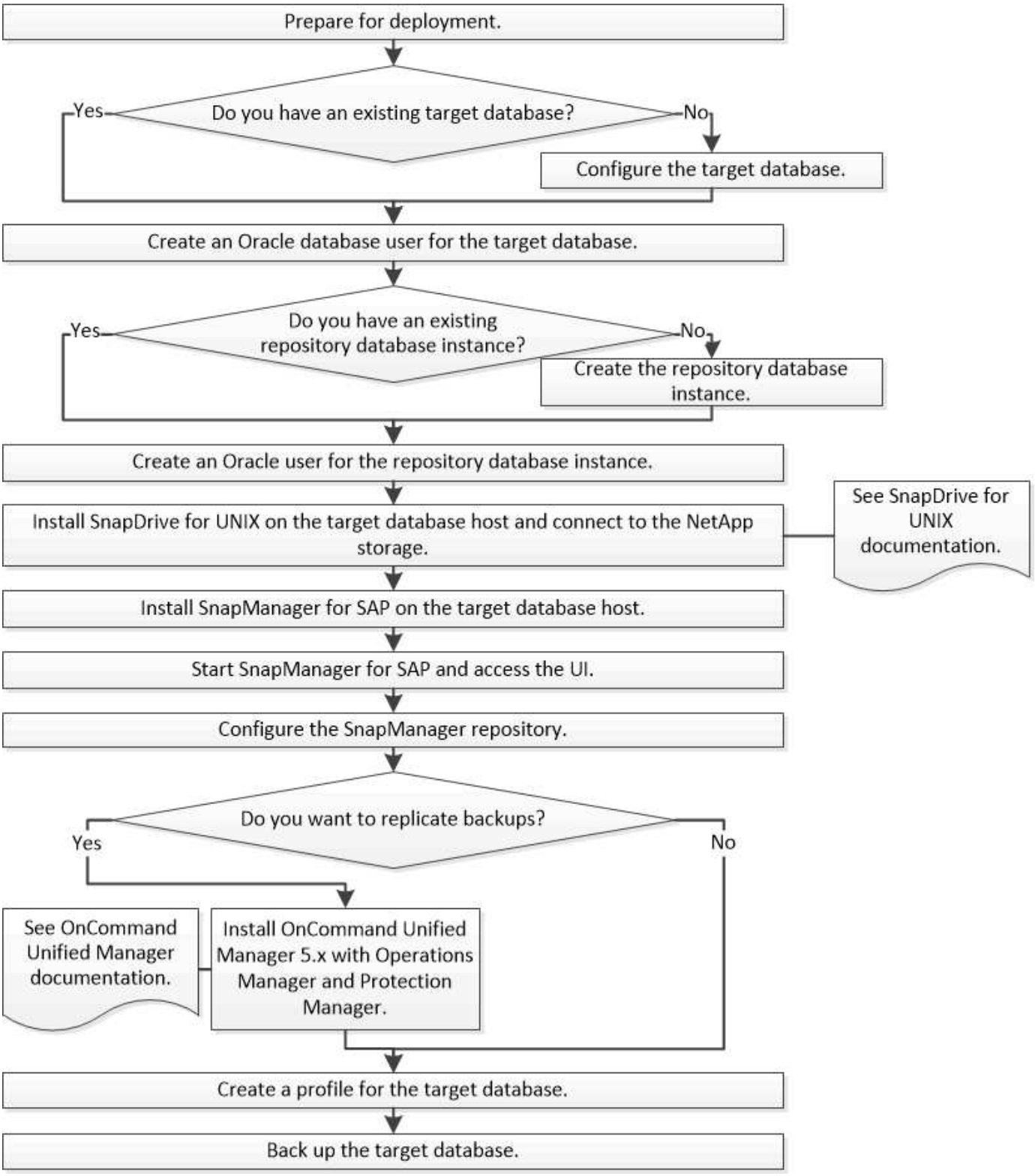
When you enable data protection on a database profile, the backups created on the primary storage system by SnapManager are replicated to a secondary NetApp storage system using SnapVault and SnapMirror technologies.

Related information

NetApp Interoperability Matrix Tool

Deployment workflow

Before you can create backups with SnapManager, you need to first install SnapDrive for UNIX and then install SnapManager for SAP.



Prepare for deployment

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 database host; and *per-storage system licensing*, in which the SnapManager license resides on the storage system.

The SnapManager license requirements are as follows:

License	Description	Where required
SnapManager per-server	A host-side license for a specific database host.Licenses are required only for database hosts on which SnapManager is installed. No SnapManager license is required for the storage system.	On the SnapManager host. A SnapManager license is not required on primary and secondary storage systems when using per-server licensing.
SnapManager per-storage system	A storage-side license that supports any number of database hosts. Required only if you are not using a per-server license on the database host.	On primary and secondary storage systems.
SnapRestore	A required license that enables SnapManager to restore databases.	On primary and secondary storage systems. Required on SnapVault destination systems to restore a file from a backup.
FlexClone	An optional license for cloning databases.	On primary and secondary storage systems.Required on SnapVault destination systems when creating clones from a backup.
SnapMirror	An optional license for mirroring backups to a destination storage system.	On primary and secondary storage systems.
SnapVault	An optional license for archiving backups to a destination storage system.	On primary and secondary storage systems.
Protocols	NFS, iSCSI, or FC license is required depending on the protocol used.	On primary and secondary storage systems. Required on SnapMirror destination systems to serve data if a source volume is unavailable.

Supported configurations

The hosts on which you are installing SnapManager must meet the specified software, browser, database, and operating system requirements. You must verify support for your configuration before you install or upgrade SnapManager.

For information about supported configurations, see the Interoperability Matrix Tool.

Related information

NetApp Interoperability Matrix Tool

Supported storage types

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

Machine	Storage type
Physical server	• NFS-connected volumes • FC-connected LUNs • iSCSI-connected LUNs
VMware ESX	• NFS volumes connected directly to the guest system • RDM LUNs on the guest operating system

UNIX host requirements

You must install SnapManager for SAP on every host where the database you want to backup is hosted. You must ensure that your hosts meet the minimum requirements for SnapManager configuration.

- You must install SnapDrive on the database host before you install SnapManager.
- You can install SnapManager either on physical or virtual machines.
- You must install the same version of SnapManager on all hosts that share the same repository.
- You must install Oracle patch `13366202` if you are using Oracle databases 11.2.0.2 or 11.2.0.3.

  If you are using DNFS, you must also install the patches listed in the My Oracle Support (MOS) report `1495104.1` for maximum performance and stability.

To use the SnapManager graphical user interface (GUI), you must have a host running on one of the following platforms. The GUI also requires that Java Runtime Environment (JRE) 1.8 is installed on the host.

- Red Hat Enterprise Linux
- Oracle Enterprise Linux
- SUSE Enterprise Linux
- Solaris SPARC, x86, and x86_64
- IBM AIX

SnapManager also operates in the VMware ESX virtualized environment.

Configure databases

Install SnapManager

Set up SnapManager

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.

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.

Backing up and verifying your databases

After installing SnapManager, you can create a basic backup of your database and verify that backup to ensure it does not contain any corrupt files.

SnapManager backup overview

SnapManager uses NetApp Snapshot technology to create backups of databases. You can use the DBVERIFY utility, or you can use SnapManager to verify the integrity of the backups.

SnapManager backs up a database by creating Snapshot copies of the volumes containing data files, control files, and archive log files. Together, these Snapshot copies comprise a backup set that SnapManager can use to restore a database.

Defining a backup strategy

Defining a backup strategy before creating your backups ensures that you have backups to successfully restore your databases. SnapManager provides flexible granular backup schedule to meet your Service Level Agreement (SLA).

For SnapManager best practices, see *TR 3761*.

What mode of SnapManager backup do you need?

SnapManager supports two modes of backups:

Backup mode	Description
Online backup	Creates a backup of the database when the database is in online state. This backup mode is also called a hot backup.
Offline backup	Creates a backup of the database when the database is either in a mounted or shutdown state. This backup mode is also called a cold backup.

What type of SnapManager backup do you need?

SnapManager supports three types of backups:

Backup type	Description
Full backup	Creates a backup of the entire database, which includes all the datafiles, control files, and archive log files.
Partial backup	Creates a backup of selected datafiles, control files, tablespaces, and archive log files

Backup type	Description
Archive log-only backup	Creates a backup of only the archive log files.You must select **Backup Archivelogs Separately** while creating the profile.

What type of database profile do you need?

SnapManager creates backups based on whether the database profile separates the archive log backups from the data file backups.

Profile type	Description
A single database profile for combined backup of data files and archive logs	Allows you to create: • Full backup containing all the data files, archive log files, and control files • Partial backup containing selected data files, tablespaces, archive log files, and control files
Separate database profiles for archive log backups and data file backups	Allows you to create: • Combined backup with different labels for data file backup and archive log backup • Data-files-only backup of all the data files along with the control files • Partial data-files-only backup of selected data files or tablespaces along with the control files • Archive-logs-only backup

What naming conventions should be used for Snapshot copies?

Snapshot copies created by backups can follow a custom naming convention. Custom text or built-in variables such as the profile name, the database name, and the database SID provided by SnapManager can be used to create the naming convention. You can create the naming convention while creating the policy.

You must include the smid variable in the naming format. The smid variable creates a unique Snapshot identifier.

The Snapshot copy naming convention can be changed during or after the creation of a profile. The updated pattern applies only to Snapshot copies that have not yet been created; existing Snapshot copies retain the previous pattern.

How long do you want to retain backup copies on the primary storage system and the secondary storage system?

A backup retention policy specifies the number of successful backups to retain. You can specify the retention policy while creating the policy.

You can select hourly, daily, weekly, monthly, or unlimited as the retention class. For each retention class, you can specify the retention count and retention duration, either together or individually.

- Retention count determines the minimum number of backups of a particular retention class that should be retained.

  For example, if backup schedule is *daily* and retention count is *10*, then 10 daily backups are retained.

  > The maximum number of Snapshot copies that Data ONTAP allows you can retain is 255. After it reaches the maximum limit, by default the creation of new Snapshot copies fail. However, you can configure the rotation policy in Data ONTAP to delete older Snapshot copies.

- Retention duration determines the minimum number of days for which the backup should be retained.

  For example, if backup schedule is *daily* and retention duration is *10*, then 10 days of daily backups are retained.

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

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

Do you want to verify backup copies using the source volume or a 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. Using a destination volume for verification reduces the load on the primary storage system.

Upgrading SnapManager

You can upgrade to the latest version of SnapManager for SAP from any of the earlier versions. You can either upgrade all the SnapManager hosts simultaneously or perform a rolling upgrade, which allows you to upgrade the hosts in a staggered, host-by-host manner.

Preparing to upgrade SnapManager

The environment in which you want to upgrade SnapManager must meet the specific software, hardware, browser, database, and operating system requirements. For the latest information about the requirements, see the Interoperability Matrix.

You must ensure that you perform the following tasks before upgrading:

- Complete the required preinstallation tasks.
- Download the latest SnapManager for SAP installation package.
- Install and configure the appropriate version of SnapDrive for UNIX on all the target hosts.
- Create a backup of the existing SnapManager for SAP repository database.

Related information

Interoperability Matrix

Post-upgrade tasks

After upgrading to a later version of SnapManager, you must update the existing repository. You might also want to modify the backup retention class assigned to the existing backupsand identify which restore process you can use.

> After upgrading to SnapManager 3.3 or later, you need to set *sqlnet.authentication_services* to **NONE** if you want to use database (DB) authentication as the only authentication method. This feature is not supported for RAC databases.

Restore process types

All restore processes are not supported in all SnapManager for SAP versions. After upgrading SnapManager, you need to be aware of the restore process that you can use for restoring a backup.

The backups that are created by using SnapManager 3.0 or later can be restored by using both fast restore and file-based restore processes. However, the backups that are created by using a version earlier than SnapManager 3.0 can be restored by using only the file-based restore process.

You can determine the SnapManager version used to create the backup by running the -backup show command.

Upgrading SnapManager hosts by using rolling upgrade

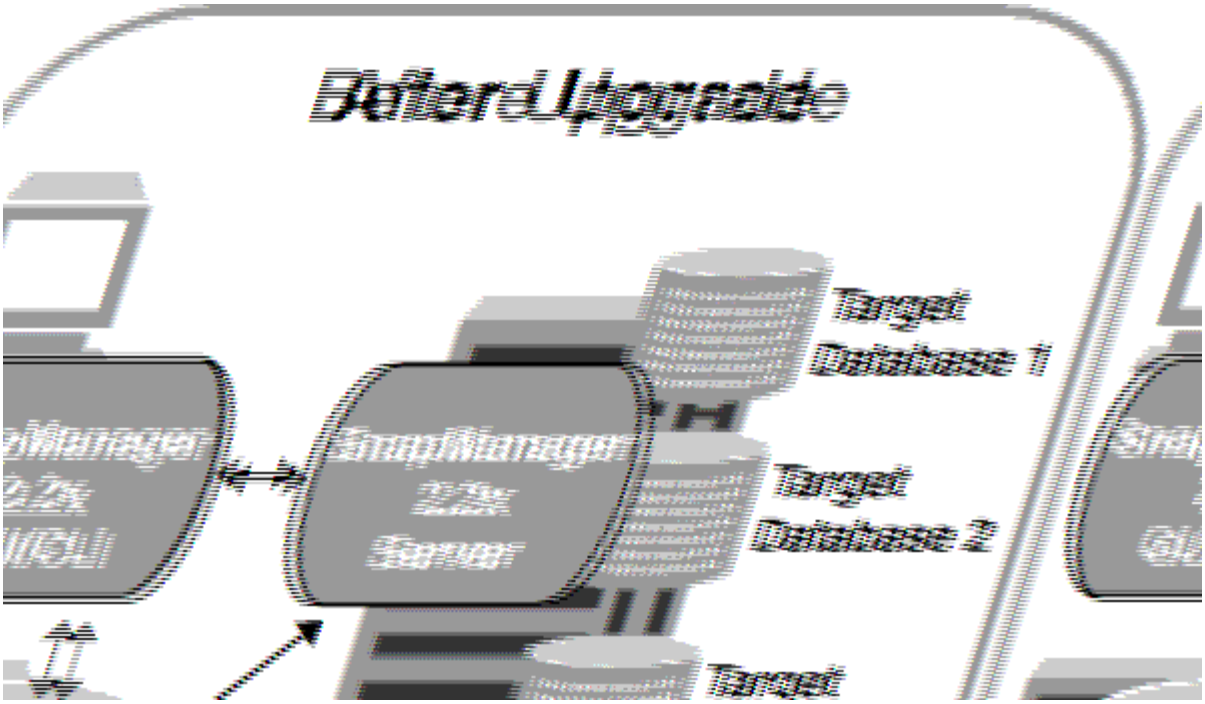
The rolling upgrade approach that enables you to upgrade the hosts in a staggered, host-by-host manner is supported from SnapManager 3.1.

SnapManager 3.0 or earlier only enabled you to upgrade all the hosts simultaneously. This resulted in downtime of all the SnapManager hosts and the scheduled operations during upgrade operation.

Rolling upgrade provides the following benefits:

- Improved SnapManager performance because only one host is upgraded at one time.
- Ability to test the new features in one SnapManager server host before upgrading the other hosts.

> You can perform rolling upgrade only by using the command-line interface (CLI).



After successful completion of rolling upgrade, the SnapManager hosts, profiles, schedules, backups, and clones associated with the profiles of the target databases are migrated from the repository database of the earlier SnapManager version to the repository database of the new version. The details about the operations performed by using the profiles, schedules, backups, and clones that were created in the earlier SnapManager version are now available in the repository database of the new version. You can start the GUI by using the default configuration values of the user.config file. The values configured in the user.config file of the earlier version of SnapManager are not considered.

The upgraded SnapManager server can now communicate with the upgraded repository database. The hosts that were not upgraded can manage their target databases by using the repository of the earlier version of SnapManager and thereby can use the features available in the earlier version.

Before performing rolling upgrade, you must ensure that all the hosts under the repository database can be resolved. For information about how to resolve the hosts, see the troubleshooting section in *SnapManager for SAP Administration Guide for UNIX*.

Related information

SnapManager 3.4.1 for SAP Administration Guide for UNIX

Prerequisites for performing rolling upgrades

Before performing a rolling upgrade, you must ensure that your environment meets certain requirements.

- If you are using any version earlier than SnapManager 3.1 and want to perform a rolling upgrade to SnapManager 3.3 or later, you need to first upgrade to 3.2 and then to the latest version.

  You can directly upgrade from SnapManager 3.2 to SnapManager 3.3 or later.

- External scripts that are used to perform any external data protection or data retention must be backed up.
- The SnapManager version to which you want to upgrade must be installed.

If you are upgrading from any version earlier than SnapManager 3.1 to SnapManager 3.3 or later, you must first install SnapManager 3.2 and perform a rolling upgrade. After upgrading to 3.2, you can then install SnapManager 3.3 or later and perform another rolling upgrade to SnapManager 3.3 or later.

- The SnapDrive for UNIX version supported with the SnapManager version to which you want to upgrade must be installed.

  The SnapDrive documentation contains details about installing SnapDrive.

- The repository database must be backed up.
- The amount of SnapManager repository utilization should be minimum.
- If the host to be upgraded is using a repository, SnapManager operations must not be performed on the other hosts that are using the same repository.

  The operations that are scheduled or running on the other hosts wait for the rolling upgrade to finish.

  It is recommended that you perform a rolling upgrade when the repository is least busy, such as over the weekend or when operations are not scheduled.

- Profiles that point to the same repository database must be created with different names in the SnapManager server hosts.

  If you use profiles with the same name, the rolling upgrade involving that repository database fails without warning.

- SnapManager operations must not be performed on the host that is being upgraded.

The rolling upgrade runs for longer as the number of backups of the hosts being upgraded together increases. The duration of the upgrade can vary depending on the number of profiles and backups associated with a given host.

Related information

Documentation on the NetApp Support Site: mysupport.netapp.com

What a rollback is

The rollback operation enables you to revert to an earlier version of SnapManager after you perform a rolling upgrade.

Before performing a rollback, you must ensure that all the hosts under the repository database can be resolved.

When you perform a rollback, the following are rolled back:

- Backups that were created, freed, and deleted by using the SnapManager version from which you are rolling back
- Clones created from a backup that was created by using the SnapManager version from which you are rolling back

- Profile credentials modified by using the SnapManager version from which you are rolling back
- Protection status of the backup modified by using the SnapManager version from which you are rolling back

The features that were available in the SnapManager version that you were using but are not available in the version to which you are rolling back, are not supported. For example, when you perform a rollback from SnapManager 3.3 or later to SnapManager 3.1, the history configuration set for profiles in SnapManager 3.3 or later is not rolled back to the profiles in SnapManager 3.1. This is because the history configuration feature was not available in SnapManager 3.1.

Limitations for performing a rollback

You must be aware of the scenarios in which you cannot perform a rollback. However, for some of these scenarios you can perform some additional tasks before performing rollback.

The scenarios in which you cannot perform rollback or have to perform the additional tasks are as follows:

- If you perform one of the following operations after performing a rolling upgrade:
  - Create a new profile.
  - Split a clone.
  - Change the protection status of the profile.
  - Assign protection policy, retention class, or SnapVault and SnapMirror relationships.

    In this scenario, after performing a rollback, you must manually remove the protection policy, retention class, or SnapVault and SnapMirror relationships that were assigned.
  - Change the mount status of the backup.

    In this scenario, you must first change the mount status to its original state and then perform a rollback.
  - Restore a backup.
  - Change the authentication mode from database authentication to operating system (OS) authentication.

    In this scenario, after performing a rollback, you must manually change the authentication mode from OS to database.
- If the host name for the profile is changed
- If profiles are separated to create archive log backups

  In this scenario, you cannot rollback to a version that is earlier than SnapManager 3.2.

Prerequisites for performing a rollback

Before performing a rollback, you must ensure that your environment meets certain requirements.

- If you are using SnapManager 3.3 or later and want to roll back to a version earlier than SnapManager 3.1, you need to roll back to 3.2 and then to the desired version.

- External scripts that are used to perform any external data protection or data retention must be backed up.
- The SnapManager version to which you want to roll back must be installed.

> If you want to perform a rollback from SnapManager 3.3 or later to a version earlier than SnapManager 3.1, you must first install SnapManager 3.2 and perform a rollback. After rolling back to 3.2, you can then install SnapManager 3.1 or earlier and perform another rollback to that version.

- The SnapDrive for UNIX version supported with the SnapManager version to which you want to roll back must be installed.

  For information about installing SnapDrive, see SnapDrive documentation set.

- The repository database must be backed up.
- If the host to be rolled back is using a repository, SnapManager operations must not be performed on the other hosts that are using the same repository.

  The operations that are scheduled or running on the other hosts wait for the rollback to complete.

- Profiles that point to the same repository database, must be created with different names in the SnapManager server hosts.

  If you use profiles with the same name, the rollback operation involving that repository database fails without warning.

- SnapManager operations must not be performed on the host which you want to rollback.

  If there is an operation running, you must wait until that operation completes and before proceeding with the rollback.

> The rollback operation runs for a longer time as the cumulative number of backups of the hosts that are being rolled back together increases. The duration of the rollback can vary depending on the number of profiles and backups associated with a given host.

Related information

Documentation on the NetApp Support Site

Post rollback tasks

You must perform some additional steps after you rollback a repository database and downgrade the SnapManager host from SnapManager 3.2 to SnapManager 3.0, to view the schedules created in the earlier version of the repository database.

1. Navigate to `cd /opt/NetApp/smsap/repositories`.

   The `repositories` directory might contain two files for each repository. The file name with the number sign (#) is created using SnapManager 3.1 or later and the file name with the hyphen (-) is created using the SnapManager 3.0.

   Example

The file names might be as follows:

- `repository#SMSAP300a#SMSAPREPO1#10.72.197.141#1521`
- `repository-smsap300a-smsaprepo1-10.72.197.141-1521`

2. Replace the number sign (#) in the file name with the hyphen (-).

   Example

   The file name that had the number sign (#), now contains hyphen (-): `repository-SMSAP300a-SMSAPREPO1-10.72.197.141-1521`.

Where to go next

After installing SnapManager and successfully creating a backup, you can use SnapManager to perform restore, recovery, and cloning operations. In addition, you might want to find information about other SnapManager features such as scheduling, managing SnapManager operations, and maintaining a history of operations.

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

- SnapManager 3.4.1 for SAP Administration Guide for UNIX

  Describes how to configure administer SnapManager for SAP. Topics include how to configure, back up, restore, and clone databases, perform secondary protection, plus an explanation of CLI commands.

- SnapManager 3.4 for SAP Release Notes

  Describes new features, fixed issues, important cautions, known issues, and limitations for SnapManager for SAP.

- *SnapManager for SAP Online Help*

  Describes the step-by-step procedures for performing different SnapManager operations using the SnapManager UI.

  > The *Online Help* is integrated with the SnapManager UI and is not available on the Support Site.

- NetApp Technical Report 3633: Best Practices for Oracle Databases on NetApp Storage

  Describes best practices to configure Oracle databases on NetApp storage system.

Related information

NetApp Support

NetApp Documentation: Product Library A-Z

Copyright information

Trademark information