Installation and Setup for UNIX for 7-mode

SnapManager for SAP

NetApp
February 20, 2023

Table of Contents

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

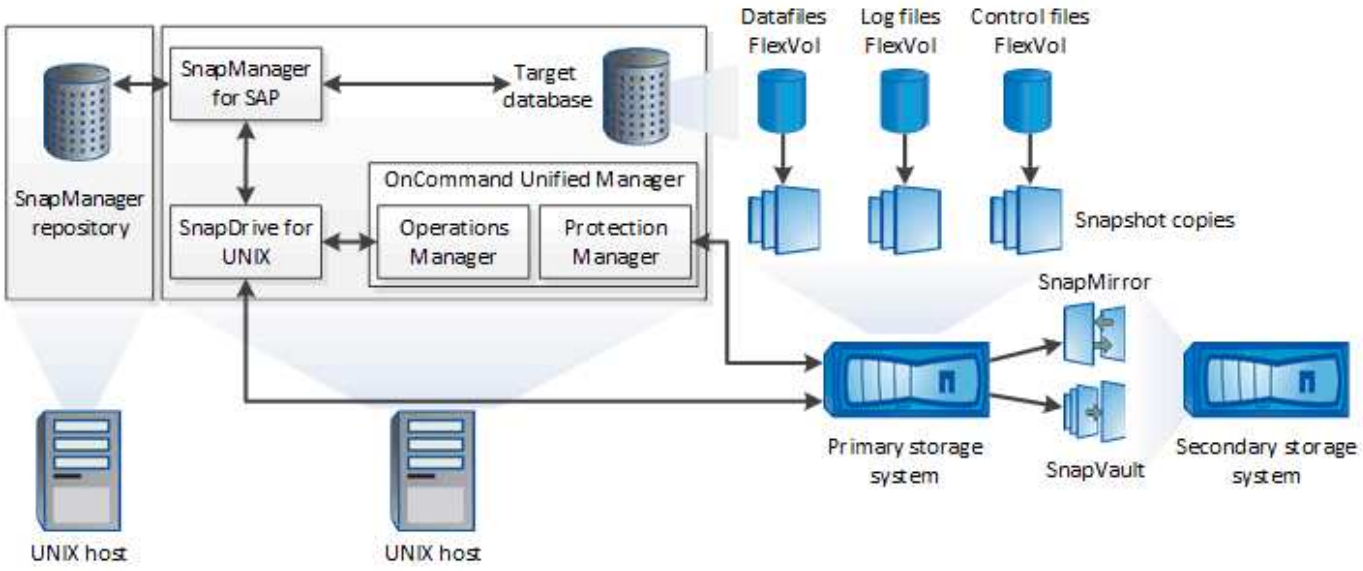
  A profile contains information about the database to be managed by SnapManager.

- 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

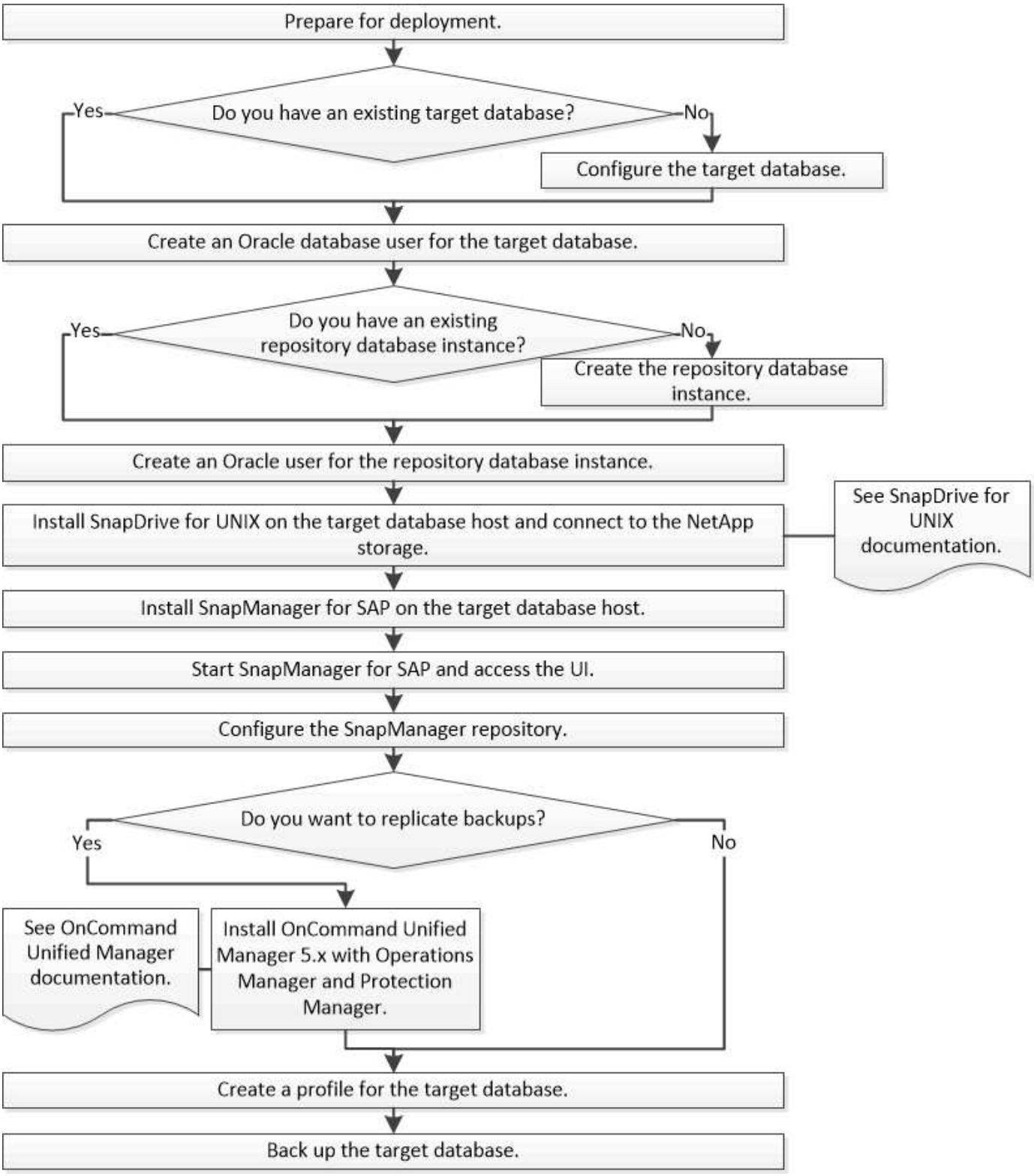
When you enable data protection on a database profile, the backups created on the primary storage system by SnapManager are replicated to a secondary NetApp storage system using SnapVault and SnapMirror technologies.

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

Before you deploy SnapManager, you must ensure your storage system and UNIX hosts meet the minimum resource requirements.

Steps

1. Verify that you have the required licenses.

2. Verify the supported configurations.
3. Verify the supported storage types.
4. Verify that your UNIX hosts meet SnapManager requirements.

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.

License	Description	Where required
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

You must configure at least two databases: a target database that you want to back up using SnapManager; and a repository database to store the target database metadata. The target database and the SnapManager repository database must be configured and online before performing SnapManager operations.

Configure the target database

The target database is an Oracle database that can be configured either as standalone, Real Application Clusters (RAC), Automatic Storage Management (ASM), or any other supported combinations.

Step

1. Configure the target database by referring to *NetApp Technical Report 3633: Best Practices for Oracle Databases on NetApp Storage*.

Related information

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

Create an Oracle database user for the target database

An Oracle database user is required to log in to the database and perform SnapManager operations. You must create this user with the *sysdba* privilege if a user with the *sysdba* privilege does not exist for the target database.

About this task

SnapManager can use any Oracle user with the *sysdba* privilege that exists for the target database. For example, SnapManager can use the default *sys* user. However, even if the user exists, you can create a new user for the target database and assign the *sysdba* privilege.

You can also use the OS authentication method wherein the operating system (OS) allows the Oracle database to use the credentials that are maintained by the OS to authenticate users to log in to the database and perform SnapManager operations. If you are authenticated by the OS, you can connect to the Oracle database without specifying a user name or password.

Steps

1. Log in to SQL *Plus:

   sqlplus '/ as sysdba'

2. Create a new user with an administrator password:

   create user *user_name* identified by *admin_password;*

   user_name is the name of the user you are creating and *admin_password* is the password that you want to assign to the user.

3. Assign the sysdba privilege to the new Oracle user:

   grant sysdba to *user_name;*

Create the repository database instance

The repository database instance is an Oracle database in which you create the SnapManager repository. The repository database instance must be a stand-alone database and cannot be the target database.

You must have an Oracle database and a user account to access the database.

1. Log in to SQL *Plus: `sqlplus '/ as sysdba'`
2. Create a new tablespace for the SnapManager repository: `create tablespacetablespace_name datafile '/u01/app/oracle/oradata/datafile/tablespace_name.dbf' size 100M autoextend on;`

   tablespace_name is the name of the tablespace.

3. Verify the block size of the tablespace: `select tablespace_name, block_size from dba_tablespaces;`

   SnapManager requires a minimum 4-K block size for the tablespace.

Related information

NetApp Technical Report 3761: SnapManager for Oracle: Best Practices

Create an Oracle user for the repository database instance

An Oracle user is required to log in to and access the repository database instance. You must create this user with *connect* and *resource* privileges.

1. Log in to SQL *Plus:

   sqlplus '/ as sysdba'

2. Create a new user and assign an administrator password to that user:

```
create user user_name identified by admin_password default tablespace
tablespace_name quota unlimited on tablespace_name;
```

- *user_name* is the name of the user you are creating for the repository database.
- *admin_password* is the password you want to assign to the user.
- *tablespace_name* is the name of the tablespace created for the repository database.

3. Assign *connect* and *resource* privileges to the new Oracle user:

```
grant connect, resource to user_name;
```

Verify the Oracle listener configuration

The listener is a process that listens for client connection requests. It receives incoming client connection requests and manages the traffic of these requests to the database. Before connecting to a target database or repository database instance, you can use the `STATUS` command to verify the listener configuration.

About this task

The `STATUS` command displays basic status information about a specific listener, including a summary of listener configuration settings, listening protocol addresses, and a summary of services registered with that listener.

1. Enter the following command at the command prompt: **`lsnrctl STATUS`**

   The default value assigned to the listener port is 1521.

Install SnapManager

You must install SnapManager on each host where the database you want to backup is running.

What you'll need

You must have installed SnapDrive for UNIX on the database host and established a connection to the storage system.

For information about how to install SnapDrive and establish connection to storage system, see SnapDrive for UNIX documentation.

About this task

You must install one SnapManager instance per database host. If you are using a Real Application Cluster (RAC) database and want to back up the RAC database, you must install SnapManager on all the hosts of the RAC database.

1. Download the SnapManager for SAP install package for UNIX from the NetApp Support Siteand copy it to the host system.

   NetApp Downloads: Software

2. Log in to the database host as the root user.
3. From the command prompt, navigate to the directory where you copied the install package.
4. Make the install package executable:

   chmod 755 ***install_package.bin***

5. Install SnapManager:

   ./install_package.bin

6. Press `Enter` to continue.
7. Perform the following steps:

   a. Change the default value of the operating system user to **ora** *sid*, where *sid* is the system identifier of the database.

   b. Press `Enter` to accept the default value for operating system group.

      The default value for the group is *dba*.

   c. Press `Enter` to accept the default value for the startup type.

   The configuration summary is displayed.

8. Review the configuration summary and press `Enter` to continue.

   SnapManager for SAP and the required Java Runtime Environment (JRE) are installed and the `smsap_setup` script is executed automatically.

   SnapManager for SAP is installed at `/opt/NetApp/smsap`.

After you finish

You can verify if the installation was successful by performing the following steps:

1. Start the for SnapManager server by running the following command:

   smsap_server start

   A message is displayed stating that the for SnapManager server is running.

2. Verify that the SnapManager for SAP for system is running correctly by entering the following command:

   smsap system verify

   The following message is displayed: Operation Id number succeeded.

   number is the operation ID number.

Related information

NetApp Documentation: SnapDrive for UNIX

Integrate with SAP BR* Tools

The SAP BR* Tools that contains SAP tools for Oracle database administration, for example, BRARCHIVE, BRBACKUP, BRCONNECT, BRRECOVER, BRRESTORE, BRSPACE, and BRTOOLS uses the BACKINT interface provided by SnapManager for SAP. To integrate SAP BR* Tools, you must create a link from the BR* Tools directory to `/opt/NetApp/smsap/bin/`, where the BACKINT file is installed.

What you'll need

- You must ensure that you have installed SAP BR* Tools.

Steps

1. Create a link from the BR*Tools directory to the `/opt/NetApp/smsap/bin/backint` file for each SAP instance.

   You must use the link instead of copying the file so that when you install a new version of SnapManager, the link will point to the new BACKINT interface version.

2. Set credentials for the user that runs the BR*Tools commands.

   The operating system user needs the credentials of the SnapManager for SAP repository, profile, and server to support the backup and restore of the SAP instance.

3. Specify a different profile name.

   By default, SnapManager uses the profile with the same name as the SAP system identifier when processing commands from BR*Tools. If this system identifier is not unique in your environment, modify the `initSID.utl` SAP initialization file, and create a parameter to specify the correct profile. The `initSID.utl` file is located at `%ORACLE_HOME%\database`.

   Example

   A sample `initSID.utl` file is as follows:

```
# Backup Retention policy.
# Specifies the retention / lifecycle of backups on the filer.
#
----------------------------------------------------------------------
----------
# Default Value: daily
# Valid Values: unlimited/hourly/daily/weekly/monthly
# retain = daily
# Enabling Fast Restore.
#
----------------------------------------------------------------------
----------
# Default Value: fallback
# Valid Values: require/fallback/off
#
# fast = fallback
# Data Protection.
#
----------------------------------------------------------------------
----------
# Default Value: empty
# Valid Values: empty/yes/no
# protect =
# profile_name = SID_BRTOOLS
```

The parameter name is always in lowercase and the comments must have a number sign (#).

4. Edit the `initSID.sap` BR*Tools configuration file by performing the following steps:
   a. Open the `initSID.sap` file.
   b. Locate the section containing the backup utility parameter file information.

      Example

      ```
      # backup utility parameter file
      # default: no parameter file
      # util_par_file =
      ```

   c. Edit the last line to include the `initSID.utl` file.

      Example

```
# backup utility parameter file
# default: no parameter file
# util_par_file = initSID.utl
```

After you finish

Register the BACKINT interface in your System Landscape Directory (SLD) by running the `backint register-sld` command.

Set up SnapManager

You can start SnapManager and access it by using either the user interface (UI) or the command-line interface (CLI). After accessing SnapManager, you must create the SnapManager repository before performing any SnapManager operations.

Start the SnapManager server

You must start the SnapManager server from the target database host.

Step

1. Log in to the target database host and start the SnapManager server:

   `smsap_server start`

   The following message is displayed: `SnapManager Server started on secure port` *`port_number with PID PID_number`*.

   > The default port is *27214*.

After you finish

You can verify that SnapManager is running correctly:

`smsap_server verify`

The following message is displayed: `Operation Id` *`operation_ID_number`* `succeeded`.

Access the SnapManager user interface

You can access the SnapManager user interface (UI) remotely by using a web browser from any system running on an operating system supported by SnapManager. You can also access the SnapManager UI from the target database host by running the `smsapgui` command.

What you'll need

- You must ensure that SnapManager is running.

- You must ensure that the supported operating system and Java are installed on the system where you want to access the SnapManager UI.

  For information about the supported operating system and Java, see the Interoperability Matrix tool.

Steps

1. In the web browser window, enter the following:

   `https://server_name.domain.com:port_number`

   - *`server_name`* is the name of the target database host where SnapManager is installed.

   You can also enter the IP address of the target database host.

   - *`port_number`* is the port on which SnapManager is running.

     The default value is 27214.

2. Click the **Launch SnapManager for SAP** link.

   The SnapManager for SAP UI is displayed.

Configure the SnapManager repository

You must configure the SnapManager repository in the repository database instance. The repository database stores metadata for databases managed by SnapManager.

What you'll need

- You must have created the repository database instance.
- You must have created the Oracle user for the repository database instance with required privileges.
- You must have included the repository database instance details in the `tnsnames.ora` file.

About this task

You can configure the SnapManager repository either from the SnapManager user interface (UI) or command-line interface (CLI). These steps show how to create a repository using the SnapManager UI. You can also use the CLI if you prefer.

For information about how to create the repository by using CLI, see the *SnapManager for SAP Administration guide for UNIX*.

1. In the left pane of the SnapManager UI, right-click **Repositories**.
2. Select **Create New Repository** and click **Next**.
3. In the **Repository Database Configuration Information** window, enter the following information:

In this field…	Do this…
User Name	Enter the name of the user you created for the repository database instance.

In this field…	Do this…
Password	Enter the password.
Host	Enter the IP address of the host where the repository database instance is created.
Port	Enter the port used to connect to the repository database instance. The default port is 1521.
Service Name	Enter the name that SnapManager uses to connect to the repository database instance. Depending on the details included in the `tnsnames.ora` file, this might be the short service name or the fully qualified service name.

4. In the **Perform Repository Add Operation** window, review the configuration summary and click **Add**.

   If the operation fails, click the **Operation Details** tab to view what caused the operation to fail. The error details are also captured in the operation log located at /var/log/smsap.

5. Click **Finish**.

   The repository is listed in the left pane under the **Repositories** tree. If you do not see the repository, right-click **Repositories** and click **Refresh**.

Related information

SnapManager 3.4.1 for SAP Administration Guide for UNIX

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.

Prepare storage systems for SnapMirror replication

Before you can use SnapManager's integrated SnapMirror technology to mirror Snapshot copies, you must configure and initialize a *data-protection relationship* between the source and destination volumes. On initialization, 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, less recent Snapshot copies on the source volume to the destination volume.

About this task

You can use the ONTAP CLI or OnCommand System Manager to perform these tasks. The procedure below is based on the assumption that you are using the CLI. For more information, see the Data ONTAP 8.2 Data Protection Online Backup and Recovery Guide for 7-Mode.

You cannot use SnapManager to mirror qtrees. SnapManager supports volume mirroring only.

You cannot use SnapManager for synchronous mirroring. SnapManager supports asynchronous mirroring only.

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.

1. On the source system console, use the `options snapmirror.access` command to specify the host names of systems that are allowed to copy data directly from the source system.

   Example

   The following entry allows replication to destination_systemB:

```
options snapmirror.access host=destination_systemB
```

2. On the destination system, create or edit the `/etc/snapmirror.conf` file to specify the volume to be copied.

   Example

   The following entry specifies replication from vol0 of source_systemA to vol2 of destination_systemB:

   ```
   source_systemA:vol0 destination_systemB:vol2
   ```

3. On both the source and destination system consoles, use the `snapmirror on` command to enable SnapMirror.

   Example

   The following command enables SnapMirror:

   ```
   snapmirror on
   ```

4. On the destination system console, use the `vol create` command to create a SnapMirror destination volume that is the same or greater in size than the source volume.

   Example

   The following command creates a 2-GB destination volume named vol2 on the aggregate aggr1:

   ```
   vol create vol2 aggr1 2g
   ```

5. On the destination system console, use the vol restrict command to mark the destination volume as restricted.

   Example

   The following command marks the destination volume vol2 as restricted:

   ```
   vol restrict vol2
   ```

6. On the source system console, use the `snap sched` command to disable any scheduled transfers.

   Example

   You must disable scheduled transfers to avoid scheduling conflicts with SnapDrive.

   The following command disables scheduled transfers:

```
snap sched vol1 -----
```

7. On the destination system console, use the `snapmirror initialize` command to create a relationship between the source and destination volumes, and 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 creates a SnapMirror relationship between the source volume vol0 on source_systemA and the destination volume vol2 on destination_systemB, and initializes the relationship:

```
snapmirror initialize -S source_systemA:vol0 destination_systemB:vol2
```

Prepare storage systems for SnapVault replication

Before you can use SnapManager's integrated SnapVault technology to archive Snapshot copies to disk, you must configure and initialize a *data-protection relationship* between the source and destination volumes. 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.

What you'll need

- You must have configured a dataset for the primary storage location in the SnapManager Configuration wizard.
- All LUNs must be in qtrees, with one LUN per qtree.

> 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.

Steps

1. On both the source and destination system consoles, enable SnapVault:

   Example

```
options snapvault.enable on
```

2. On the source system console, use the `options snapvault.access` command to specify the host names of systems that are allowed to copy data directly from the source system.

   Example

The following command allows replication to destination_systemB:

```
options snapvault.access host=destination_systemB
```

3. On the destination system console, use the `options snapvault.access` command to specify the host names of systems to which copied data can be restored.

   Example

   The following command allows copied data to be restored to source_systemA:

   ```
   options snapvault.access host=destination_systemA
   ```

4. On the source system console, use the `ndmpd on` command to enable NDMP.

   Example

   The following command enables NDMP:

   ```
   ndmpd on
   ```

5. On the destination system console, use the `vol create` command to create a SnapMirror destination volume that is the same or greater in size than the source volume.

   Example

   The following command creates a 2-GB destination volume named vol2 on the aggregate aggr1:

   ```
   vol create vol2 aggr1 2g
   ```

6. In the OnCommand Unified Manager (UM) NetApp Management Console, add the resource pool for the destination volume:
   a. Click **Data** > **Resource Pools** to open the **Resource Pools** page.
   b. On the Resource Pools page, click **Add** to start the **Add Resource Pool** wizard.
   c. Follow the prompts in the wizard to specify the aggregate for the destination volume.
   d. Click **Finish** to exit the wizard.
7. In the UM NetApp Management Console, assign the resource pool to the dataset you created in the SnapManager Configuration wizard:
   a. Click **Data** > **Datasets** to open the Datasets page.
   b. On the **Datasets** page, select the dataset you created and click **Edit**.
   c. On the **Edit Dataset** page, click **Backup** > **Provisioning/Resource Pools** to open the **Configure Dataset Node** wizard.
   d. Follow the prompts in the wizard to assign the resource pool to the dataset.

Resource pool assignment specifies the data-protection relationship between the source and destination volumes.

e. Click **Finish** to exit the wizard and initialize the data-protection relationship.

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

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
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.

Related information

NetApp Technical Report 3761: SnapManager for Oracle: Best Practices

Create a profile for your database

You must create a profile for your database to perform any operation on that database. The profile contains information about the database and can reference only one database; however, a database can be referenced by multiple profiles. A backup that is created using one profile cannot be accessed from a different profile, even if both profiles are associated with the same database.

What you'll need

You must ensure that target database details are included in the `/etc/oratab` file.

About this task

These steps show how to create a profile for your database using the SnapManager UI. You can also use the CLI if you prefer.

For information about how to create profiles using the CLI, see the *SnapManager for SAP Administration guide for UNIX*.

Steps

1. From the Repositories tree, right-click the repository or the host and select **Create Profile**.
2. On the **Profile Configuration Information** page, enter the custom name and password for the profile.
3. On the **Database Configuration Information** page, enter the following information:

In this field…	Do this…
Database Name	Enter the name of the database you want to backup.
Database SID	Enter the secure ID (SID) of the database. The database name and the database SID can be the same.
Host	Enter the IP address of the host where the target database resides. You can also specify the host name if the host name is specified in the Domain Name System (DNS).
Host Account	Enter the Oracle user name of the target database. The default value for the user is oracle.
Host Group	Enter the Oracle user group name. The default value is dba.

4. On the Database Connection Information page, select one of the following:

Choose this…	If you want to…
Use O/S Authentication	Use the credentials maintained by the operating system to authenticate users who access the database.
Use Database Authentication	Allow Oracle to authenticate an administrative user using password file authentication. Enter the appropriate database connection information. • In the **SYSDBA Privileged User Name** field, enter the name of the database administrator with administrative privileges. • In the **Password** field, enter the password of the database administrator. • In the **Port** field, enter the port number used to connect to the host where the database resides. The default value is 1527.

Choose this…	If you want to…
Use ASM Instance Authentication	Allow Automatic Storage Management (ASM) database instance to authenticate an administrative user. Enter the appropriate ASM instance authentication information. • In the **SYSDBA/SYSASM Privileged User Name** field, enter the user name of the ASM instance administrator with administrative privileges. • In the **Password** field, enter password of the administrator.

You can select the ASM authentication mode only if you have an ASM instance on the database host.

5. On the RMAN Configuration Information page, select one of the following:

Choose this…	If…
Do not use RMAN	You are not using RMAN to manage backup and restore operations.
Use RMAN via the control file	You are managing the RMAN repository using control files.
Use RMAN via Recovery Catalog	You are managing the RMAN repository using recovery catalog database. Enter the user name who has access to recovery catalog database, password, and the Oracle net service name of the database that manages the Transparent Network Substrate (TNS) connection.

6. On the **Snapshot Naming Information** page, select the variables to specify a naming format for the Snapshot copy.

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

7. On the **Policy Settings** page, perform the following:
   a. Enter the retention count and duration for each retention class.
   b. From the **Protection Policy** drop-down list, select the Protection Manager policy.
   c. If you want to back up archive logs separately, select the **Backup Archivelogs Separately** checkbox, specify the retention, and select the protection policy.

      You can select a policy which is different from the policy associated for datafiles. For example, if you have selected one of the Protection Manager policy for datafiles, you can select a different Protection Manager policy for archive logs.

8. On the **Configure Notification Settings** page, specify the email notification settings.
9. On the **History Configuration Information** page, select one of the options to maintain the history of SnapManager operations.

10. On the **Perform Profile Create Operation** page, verify the information and click **Create**.
11. Click **Finish** to close the wizard.

    If the operation fails, click **Operation Details** to view what caused the operation to fail.

Related information

SnapManager 3.4.1 for SAP Administration Guide for UNIX

Back up your database

After creating a profile, you must back up your database. You can schedule recurring backups after the initial backup and verification.

About this task

These steps show how to create a backup of your database using the SnapManager user interface. You can also use the command-line interface (CLI) if you prefer.

For information about how to create backups using the CLI or SAP BR* Tools, see the *SnapManager for SAP Administration guide for UNIX*.

Steps

1. From the Repositories tree, right-click the profile containing the database you want to back up, and select **Backup**.
2. In **Label**, enter a custom name for the backup.

   You must not include spaces or special characters in the name. If you do not specify a name, SnapManager automatically creates a backup label.

   From SnapManager 3.4, you can modify the backup label created automatically by SnapManager. You can edit the `override.default.backup.pattern` and `new.default.backup.pattern` configuration variables to create your own default backup label pattern.

3. Select **Allow startup or shutdown of database, if necessary** to modify the state of the database, if required.

   This option ensures that if the database is not in the required state to create a backup, SnapManager automatically brings the database to the desired state to complete the operation.

4. On the **Database, Tablespaces or Datafiles to Backup page**, perform the following:
   a. Select **Backup Datafiles** to back up either the full database, selected data files, or selected tablespaces.
   b. Select **Backup Archivelogs** to back up the archive log files separately.
   c. Select **Prune Archivelogs** if you want to delete the archive log files from the active file system that is already backed up.

      If Flash Recovery Area (FRA) is enabled for archive log files, then SnapManager fails to prune the archive log files.

   d. Select **Protect the backup** if you want to enable backup protection.

This option is enabled only if the protection policy was selected while creating the profile.

e. Select **Protect Now** if you want to protect the backup immediately to the secondary storage overriding Protection Manager's protection schedule.

f. From the **Type** drop-down list, select the type of backup (offline or online) you want to create.

If you select *Auto*, SnapManager creates a backup based on the current state of the database.

g. From the **Retention Class** drop-down list, select the retention class.

h. Select the **Verify backup using the Oracle DBVERIFY utility** check box if you want to ensure that the backed-up files are not corrupted.

5. On the **Task Enabling** page, specify whether you want to perform tasks before and after backup operations are completed.
6. On the **Perform Backup Operation** page, verify the information and click **Backup**.
7. Click **Finish** to close the wizard.

If the operation fails, click **Operation Details** to view what caused the operation to fail.

Related information

SnapManager 3.4.1 for SAP Administration Guide for UNIX

Verify database backups

You can verify the backup of your database to ensure that the backed-up files are not corrupted.

About this task

If you did not select the **Verify backup using the Oracle DBVERIFY utility** check box while creating a backup, you must perform these steps manually to verify the backup. However, if you selected the check box, SnapManager automatically verifies the backup.

Steps

1. From the **Repositories** tree, select the profile.
2. Right-click the backup that you want to verify, and select **Verify**.
3. Click **Finish**.

If the operation fails, click **Operation Details** to view what caused the operation to fail.

In the **Repository** tree, right-click the backup, and then click **Properties** to view the results of the verify operation.

After you finish

You can use backed-up files to perform restore operations. For information about how to perform restore operations using the SnapManager user interface (UI), see the *Online Help*. If you want to use the command-line interface (CLI) to perform restore operations, see the *SnapManager for SAP Administration guide for UNIX*.

Related information

SnapManager 3.4.1 for SAP Administration Guide for UNIX

Schedule recurring backups

You can schedule backup operations so that the backups are initiated automatically at regular intervals. SnapManager allows you to schedule backups on an hourly, daily, weekly, monthly, or one-time basis.

About this task

You can assign multiple backup schedules for a single database. However, when scheduling multiple backups for the same database, you must ensure that the backups are not scheduled at the same time.

These steps show how to create a backup schedule for your database using the SnapManager user interface (UI). You can also use the command-line interface (CLI) if you prefer. For information about how to schedule backups using the CLI, see the *SnapManager for SAP Administration guide for UNIX*.

1. From the Repositories tree, right-click the profile containing the database for which you want to create a backup schedule, and select **Schedule Backup**.
2. In **Label**, enter a custom name for the backup.

   You must not include spaces or special characters in the name. If you do not specify a name, SnapManager automatically creates a backup label.

   From SnapManager 3.4, you can modify the backup label created automatically by SnapManager. You can edit the `override.default.backup.pattern` and `new.default.backup.pattern` configuration variables to create your own default backup label pattern.

3. Select **Allow startup or shutdown of database, if necessary** to modify the state of the database, if required.

   This option ensures that if the database is not in the required state to create a backup, SnapManager automatically brings the database to the desired state to complete the operation.

4. On the **Database, Tablespaces or Datafiles to Backup** page, perform the following:
   a. Select **Backup Datafiles** to back up either the full database, selected data files, or selected tablespaces.
   b. Select **Backup Archivelogs** to back up the archive log files separately.
   c. Select **Prune Archivelogs** if you want to delete the archive log files from the active file system that is already backed up.

      If Flash Recovery Area (FRA) is enabled for archive log files, then SnapManager fails to prune the archive log files.

   d. Select **Protect the backup** if you want to enable backup protection.

      This option is enabled only if the protection policy was selected while creating the profile.

   e. Select **Protect Now** if you want to protect the backup immediately to the secondary storage overriding Protection Manager's protection schedule.

f. From the **Type** drop-down list, select the type of backup (offline or online) you want to create.

   If you select *Auto*, SnapManager creates a backup based on the current state of the database.

g. From the **Retention Class** drop-down list, select the retention class.

h. Select the **Verify backup using the Oracle DBVERIFY utility** check box if you want to ensure that the backed-up files are not corrupted.

5. In the **Schedule Name** field, enter a custom name of the schedule.

   You must not include spaces in the name.

6. On the **Configure Backup Schedule** page, perform the following:
   a. From the **Perform this operation** drop-down list, select the frequency of the backup schedule.
   b. In the **Start Date** field, specify the date when you want to initiate the backup schedule.
   c. In the **Start Time** field, specify the time when you want to initiate the backup schedule.
   d. Specify the interval in which backups will be created.

      For example, if you have selected the frequency as hourly and specify the interval as 2, then backups will be scheduled every 2 hours.

7. On the **Task Enabling** page, specify whether you want to perform tasks before and after backup operations are completed.
8. On the **Perform Backup Schedule Operation** page, verify the information and click **Schedule**.
9. Click **Finish** to close the wizard.

   If the operation fails, click **Operation Details** to view what caused the operation to fail.

Related information

SnapManager 3.4.1 for SAP Administration Guide for UNIX

Uninstall the software from a UNIX host

If you no longer need the SnapManager software, you can uninstall it from the host server.

Steps

1. Log in as root.
2. To stop the server, enter the following command: **`smsap_server stop`**
3. To remove the SnapManager software, enter the following command:

   `UninstallSmsap`

4. After the introduction text, press **Enter** to continue.

   The uninstallation completes.

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

Upgrade the SnapManager hosts

You can upgrade all of the existing hosts to use the latest version of SnapManager. All of the hosts are upgraded simultaneously. However, this might result in downtime of all the SnapManager hosts and the scheduled operations during that time.

Steps

1. Log in to the host system as the root user.
2. From the command-line interface (CLI), navigate to the location where you have downloaded the installation file.
3. If the file is not executable, change the permissions: **`chmod 544 netapp.smsap*`**
4. Stop the SnapManager server:

   `smsap_server stop`

5. Depending on the UNIX host, install SnapManager:

If the operating system is…	Then run…
Solaris (SPARC64)	**`# ./netapp.smsap.sunos-sparc64-version_number.bin`**
Solaris (x86_64)	**`# ./netapp.smsap.sunos-x64-version_number.bin`**

If the operating system is…	Then run…
AIX (PPC64)	`# ./netapp.smsap.aix-ppc64-version_number.bin`
Linux x86	`# ./netapp.smsap.linux-x86-version_number.bin`
Linux x64	`# ./netapp.smsap.linux-x64-version_number.bin`

6. On the **Introduction** page, press **Enter** to continue.

   The following message is displayed: `Existing SnapManager For SAP Detected.`

7. Press **Enter**.
8. At the command prompt, perform the following:

   a. Change the default value of the operating system user to **ora** *sid*.

      sid is the system identifier of the SAP database.

   b. Enter the correct value for the operating system group or press **Enter** to accept the default value.
   c. Enter the correct value for the server startup type or press **Enter** to accept the default value.

   The configuration summary is displayed.

9. Press **Enter** to continue.

   The following message is displayed: `Uninstall of Existing SnapManager For SAP has started.`

   The uninstallation is completed and the latest version of SnapManager is installed.

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.

Update the existing repository

You do need not to update the existing repository if you are upgrading from SnapManager 3.3.x to SnapManager 3.4 or later, but for all other upgrade paths you must update the existing repository so that you can access it after the upgrade.

What you'll need

- The upgraded SnapManager server must have been started and verified.
- A backup of the existing repository must exist.

About this task

- If you are upgrading from any version earlier than SnapManager 3.1 to SnapManager 3.3 or later, you must first upgrade to SnapManager 3.2.

  After upgrading to SnapManager 3.2, you can then upgrade to SnapManager 3.3 or later.

- After you update the repository, you cannot use the repository with an earlier version of SnapManager.

Step

1. Update the existing repository:

   `smsap repository update -repository -dbname repository_service_name -host repository_host_name -login -username repository_user_name -port repository_port`

   - The repository user name, repository service name, and repository host name can consist of alphanumeric characters, a minus sign, an underscore, and a period.
   - The repository port can be any valid port number. The other options used while updating the existing repository are as follows:
   - The `force` option
   - The `noprompt` option
   - The `quiet` option
   - The `verbose` option

     Example

     ```
     smsap repository update -repository -dbname HR1
     -host server1 -login -username admin -port 1521
     ```

After you finish

Restart the SnapManager server to restart any associated schedules.

Modify the backup retention class

After upgrading, SnapManager assigns the default backup retention class to the existing backups. You can modify the default retention class values to meet your backup requirements.

About this task

The default backup retention class assigned to the existing backups are as follows:

Backup type	Retention class assignment after upgrade
Backups to be retained forever	Unlimited
Other backups	Daily

You can delete the backups that are retained forever without changing the retention class.

If you upgrade to SnapManager 3.0 or later, the greater of the following two values are assigned to the existing profiles:

- Previous retention count for the profile
- Default values for the retention count and duration of daily backups as specified in the `smsap.config` file

Step

1. Modify the values assigned to `retain.hourly.count` and `retain.hourly.duration` in the `smsap.config` file.

   The `smsap.config` file is located at *`default installation location`*`/properties/smsap.config`.

   You can enter the following values:

   - retain.hourly.count = **`12`**
   - retain.hourly.duration = **`2`**

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

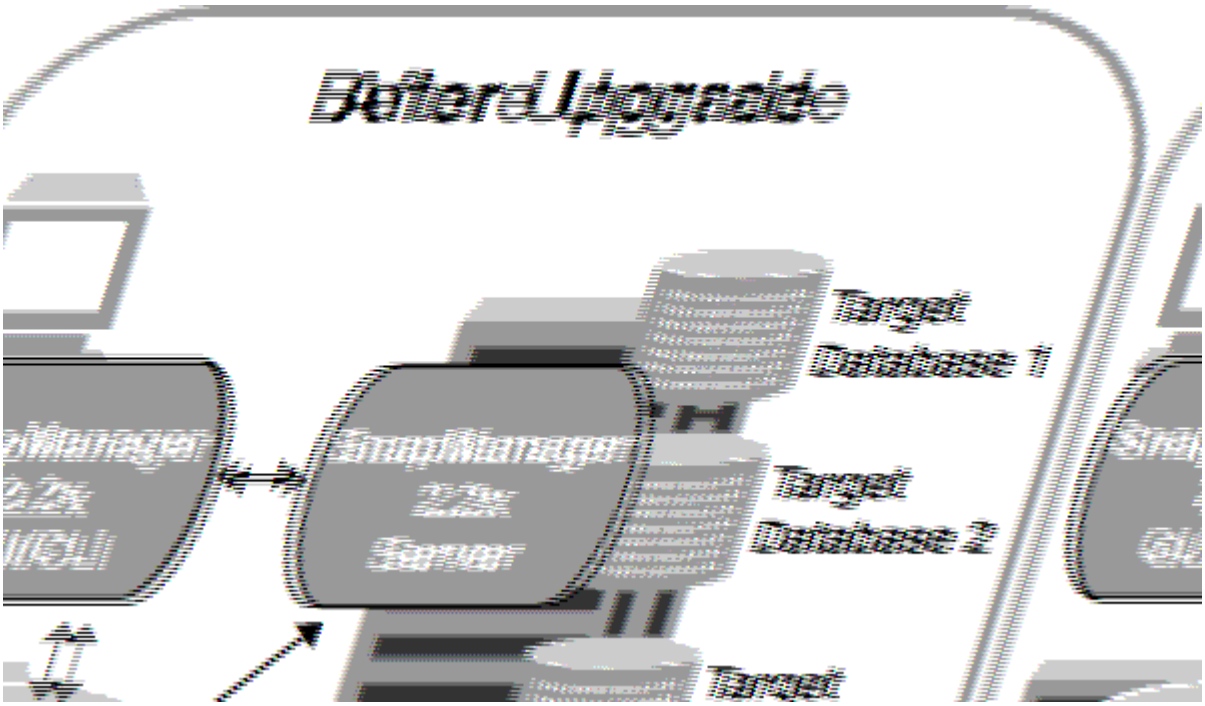
The rolling upgrade approach that enables you to upgrade the hosts in a staggered, host-by-host manner is supported from SnapManager 3.1.

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

Perform rolling upgrade on a single host or multiple hosts

You can perform rolling upgrade on a single or multiple SnapManager server hosts by using the command-line interface (CLI). The upgraded SnapManager server host is then managed only with the later version of SnapManager.

What you'll need

You must ensure that all the prerequisites for performing rolling upgrade are completed.

Steps

1. To perform a rolling upgrade on a single host, enter the following command:

   smsap repository rollingupgrade-repository-dbname *repo_service_name* -host *repo_host* -login-username *repo_username* -port *repo_port* -upgradehost *host_with_target_database* -force [-quiet | -verbose]

   The following command performs the rolling upgrade of all target databases mounted on hostA and a repository database named repoA located on repo_host:

   ```
   smsap repository rollingupgrade
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -upgradehost hostA
   ```

2. To perform a rolling upgrade on multiple hosts, enter the following command: `smsaprepository rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_port-upgradehosthost_with_target_database1,host_with_target_database2-force [-quiet | -verbose]`

   > For multiple hosts, enter the host names separated by a comma and ensure that you do not include any space between the comma and the next host name.If you are using a Real Application Clusters (RAC) configuration, you must manually upgrade all RAC-associated hosts. You can use -allhosts to perform the rolling upgrade of all the hosts.

   The following command performs the rolling upgrade of all the target databases mounted on the hosts, hostA and hostB and a repository database named repoA located on repo_host:

   ```
   smsap repository rollingupgrade
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -upgradehost hostA,hostB
   ```

3. To perform a rolling upgrade on all the hosts on a repository database, enter the following command: `smsaprepository rollingupgrade-repository-dbnamerepo_service_name-hostrepo_host-login-usernamerepo_username-portrepo_port-allhosts-force [-quiet | -verbose]`

   After successfully upgrading the repository database, you can perform all the SnapManager operations on

the target database.

The following command performs the rolling upgrade of all the target databases available on a repository database named repoA located on repo_host:

```
smsap repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
      -allhosts
```

- If the SnapManager server starts automatically, you must restart the server to ensure that you can view the schedules.
- If you upgrade one of the two related hosts, you must upgrade the second host after upgrading the first.

  For example, if you have created a clone from host A to host B or mounted a backup from host A to host B, the hosts A and B are related to each other. When you upgrade host A, a warning message is displayed asking you to upgrade the host B soon after upgrading host A.

  The warning messages are displayed even though the clone is deleted or the backup is unmounted from host B during the rolling upgrade of host A. This is because metadata exists in the repository for the operations performed on the remote host.

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

Perform a rollback on a single host or multiple hosts

You can perform a rollback on a single or multiple SnapManager server hosts by using the command-line interface (CLI).

What you'll need

You must ensure that all the prerequisites for performing a rollback are complete.

Steps

1. To perform a rollback on a single host, enter the following command:

   ```
   smsaprepository rollback-repository-dbname repo_service_name -host repo_host
   -login -username repo_username -port repo_port -rollbackhost
   host_with_target_database
   ```

   Example

   The following example shows the command to roll back all the target databases that are mounted on hostA and a repository database named repoA located on the repository host, repo_host:

```
smsap repository rollback
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -rollbackhost hostA
```

2. To perform a rollback on multiple hosts, enter the following command:

   smsaprepository rollback-repository-dbname *repo_service_name* -host *repo_host* -login-username *repo_username* -port *repo_port* -rollback *hosthost_with_target_database1,host_with_target_database2*

   For multiple hosts, enter the host names separated by a comma and ensure that there is no space between the comma and the next host name.

   If you are using Real Application Clusters (RAC) configuration, you must manually roll back all RAC-associated hosts. You can use -allhosts to perform a rollback of all the hosts.

   Example

   The following example shows the command to roll back all the target databases that are mounted on the hosts, hostA, hostB, and a repository database named repoA located on the repository host, repo_host:

```
smsap repository rollback
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -rollbackhost hostA,hostB
```

   The hosts, profiles, schedules, backups, and clones that are associated with the profiles of the target databases for the host are reverted to the earlier repository.

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 3761: SnapManager for Oracle: Best Practices

  Describes SnapManager for Oracle best practices.

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

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

- NetApp Technical Report 3442: SAP with Oracle on UNIX and NFS and NetApp Storage

  Describes best practices for deploying NetApp storage to support SAP solutions.

Related information

NetApp Support

NetApp Documentation: Product Library A-Z

Copyright information

Trademark information