Abstract
Backup, recovery, and cloning are complicated tasks that are synonymous with Oracle Database management. NetApp® SnapManager® for Oracle (SMO) management software simplifies and automates these complex operations. It does this by leveraging NetApp Snapshot®, SnapRestore®, and FlexClone® technologies to provide fast, space-efficient, disk-based backups; rapid, granular restore and recovery; and quick, space-efficient cloning of Oracle Databases. This document describes the best practices for deploying and using SnapManager 3.4 for Oracle.
Table 6) SMO configuration and creation of profile. .................................................................26
Table 7) Backup and cloning operation with protection. ............................................................32

LIST OF FIGURES
Figure 1) SnapManager for Oracle architecture. ........................................................................8
Figure 2) Example layout of a SnapManager for Oracle repository. ............................................15
Figure 3) SMO clone management for upgrading. .......................................................................23
Figure 4) Intercluster peering. ...................................................................................................25
Figure 5) Protection relationship state. .........................................................................................25
1 Introduction

In today’s data-driven enterprise, business-critical Oracle Databases must be operational around the clock to facilitate decision making, e-commerce, and myriad other business processes. Rapid growth in data volumes and database demands makes it increasingly difficult to provide availability and protection of valuable data assets. Oracle Database administrators need tools that empower them to take frequent backups with minimal operational impact, perform quick database recovery, and rapidly create clones for user testing and development.

NetApp SnapManager for Oracle (SMO) automates and simplifies the manual, complex, and time-consuming processes associated with the backup, recovery, and cloning of Oracle Databases. SnapManager leverages NetApp technologies, such as Snapshot, SnapRestore, and FlexClone, with support for the latest Oracle Database releases. SnapManager also integrates seamlessly with native Oracle technologies such as Oracle Real Application Clusters (Oracle RAC), Direct NFS, and Automatic Storage Management (ASM) across FC, iSCSI, and NFS protocols. This integration allows IT organizations to scale their storage infrastructure, meet increasingly stringent service-level-agreement commitments, and improve the productivity of database and storage administrators across the enterprise. Backups created by using SMO can optionally be cataloged with Oracle Recovery Manager (RMAN) to preserve the backup information. They can be used later in functions such as block-level restore or tablespace point-in-time recovery.

1.1 Purpose and Scope

This report describes best practices for deploying and using SnapManager 3.4 for Oracle to back up, restore, and clone Oracle Databases running on NetApp storage systems. The recommendations in this report are generic; they are not specific to any configuration. This report explains the scenarios relevant to storage running the NetApp clustered Data ONTAP® operating system.

For general guidance on best practices for Oracle on NetApp storage, refer to NetApp technical report, Oracle Databases on Data ONTAP | TR-3633.

1.2 Intended Audience

This report is intended for Oracle Database administrators, storage administrators, and architects implementing backup, recovery, and cloning solutions for Oracle Databases running on NetApp storage. Readers should have a thorough understanding of the architecture, administration, backup, and recovery concepts of Oracle Databases and should have reviewed the following documents:

- Clustered Data ONTAP 8.3 System Administration Guide for Cluster Administrators
- SnapManager 3.4 for Oracle Installation and Setup Guide for UNIX for Clustered Data ONTAP
- SnapManager 3.4 for Oracle Administration Guide for UNIX
- SnapManager 3.4 for Oracle Release Notes
- SnapDrive 5.3 for UNIX Administration Guide (if Oracle is on any variety of UNIX)
- SnapDrive for Windows for Clustered Data ONTAP Used in SAN Environments Best Practice Guide | TR-4228 (if Oracle is on Microsoft Windows)
- OnCommand Unified Manager Installation and Setup Guide
- TR-3633: Best Practice for Oracle Databases on NetApp Storage
- Oracle Dev/Test on VMware vSphere and NetApp Storage Solutions Overview

1.3 Note for 7-Mode Data ONTAP Users

The replicated data protection approach discussed in this report is specific to clustered Data ONTAP storage users. Those using Data ONTAP operating in 7-Mode should refer to policy-based data protection, which is discussed in SnapManager 3.4 for Oracle Administration Guide for UNIX.
2 SnapManager for Oracle Simplifies Oracle Database Management

2.1 Overview

This subsection provides a brief overview of some of the features in version 3.4. For a complete list of new features and enhancements, see the SnapManager 3.4 for Oracle Release Notes.

- **Support for Oracle Database 12c.** This release provides support for Oracle Database 12c, but not pluggable database (PDB) or container database (CDB) modes of operation. It does, however, provide an upgrade path for customers who want to migrate their databases from releases earlier than 12c and who want to use the basic functionality of 12c.

- **Support for NetApp SnapMirror® and SnapVault® technologies in clustered Data ONTAP.** SnapManager 3.4 for Oracle supports secondary data protection to replicate the backup Snapshot copies. It has built-in scripts to issue SnapMirror update commands at the storage level and works purely on the replication relationships defined at the Data ONTAP level. This native feature is not available in Data ONTAP operating in 7-Mode when NetApp OnCommand® Unified Manager is used for data protection.

- **Support for ASM on Linux without the use of ASMLib.** SnapManager 3.4 and later versions for Oracle now include support for ASM for Linux with and without the use of ASMLib. Oracle no longer provides ASMLib kmod binaries for Red Hat Enterprise Linux 6.0 and later versions. These binaries can be downloaded only from the Red Hat Customer Portal. Alternatively, udev rules can be used in place of ASMLib.

- **Transition support for Data ONTAP 7-Mode to clustered Data ONTAP.** SnapManager 3.4 for Oracle on clustered Data ONTAP can also recognize backup Snapshot copies that were created using Data ONTAP operating in 7-Mode. This feature is available, with certain limitations, following the transition process by using the 7-Mode Transition Tool (7MTT). Limitations are identified in the 7MTT release notes.

- **Support for the latest versions of clustered Data ONTAP and host operating system.** SnapManager 3.4 for Oracle supports clustered Data ONTAP 8.3.x versions so that users can leverage the latest features provided by Data ONTAP. SnapManager 3.4 for Oracle is qualified to work on RHEL / OL 7.x operating system.

Repository and Profiles

SnapManager organizes information about target databases as profiles in a repository. These profiles hold information about the database being managed, including its credentials, backups, and clones. The repository holds data about the operations performed on the profiles. The SnapManager repository records information such as when a backup was created, which files were backed up, and whether a clone was created by using the backups. The repository can be created by using the SnapManager GUI or command-line interface (CLI), and it resides inside an Oracle Database.

A profile must be created for each database to be managed by SnapManager. After a profile is created for a database, information that is specific to that database is stored in the repository. Once a profile is created, it is not necessary to specify the database details each time an operation is performed on that database. A profile can reference only one database; however, a database can be referenced by multiple profiles. A backup that is created by using one profile cannot be accessed from a different profile, even if both profiles are associated with the same database.

Profiles enable you to select required protection policies for backups and archive logs separately. SnapManager_cDOT_Vault and SnapManager_cDOT_Mirror are two built-in protection policies that can be used to replicate Snapshot copies using SnapVault and SnapMirror, respectively. The protection status turns to "Conformant" immediately after you create the profile until the first backup is triggered.
**Backup Retention Policy**

Users can specify the number of backups to be retained in a database when creating the SnapManager profile for that database. They also have the option to exclude a backup from the retention policy. The retention policy is engaged every time a new backup is taken and applies only to successful backups. For example, unsuccessful or failed backups and backups that are used to create a clone do not count toward retention limits. For more information, see "How SnapManager Retains Backups on the Local Storage" in the [SnapManager 3.4 for Oracle Administration Guide](#).

When creating a profile in SMO 3.4, configuring secondary data protection results in the automatic replication of backups to secondary storage. The database administrator uses SnapManager to specify only the retention and scheduling of backups on primary storage. The replication to secondary is automatically performed by SnapManager after verifying the relationship among the secondary volumes at the storage end.

**Note:** For 7-Mode storage, OnCommand Unified Manager is required to enable secondary protection.

**Protection Policies**

Protection policies are rules that govern how database backups are created and protected at the storage level by enabling replication relationships with secondary volumes in another storage virtual machine (SVM). SMO 3.4 has two built-in protection policies, SnapManager_cDOT_Mirror and SnapManager_cDOT_Vault, that mirror or vault the backup Snapshot copies to secondary storage.

A protection policy defines the following parameters:

- When to transfer copies to secondary storage
- The maximum amount of data to be transferred at scheduled times
- How long to retain Snapshot copies in the secondary location
- Warning and error thresholds for lag times

**Note:** OnCommand Unified Manager is applicable only for Data ONTAP operating in 7-Mode.

**Protected Backups**

SnapManager for Oracle creates backups and protects them on secondary storage by enabling this option during the backup. The profile controls the exact data protection relationship type. Protection is confirmed when the status of the backup shows as Protected, or by confirming the green icon across each backup label.

**Oracle Automatic Storage Management Integration**

SnapManager for Oracle in UNIX environments is seamlessly integrated with Oracle ASM. In an ASM configuration, multiple ASM disks are aggregated into a single ASM disk group. Oracle ASM lays out a file system within the ASM disk group. A single ASM-based file, therefore, can have blocks spread across multiple storage devices.

SMO can back up a database hosted on an ASM disk group even if it spans multiple storage volumes. It does this by taking a consistency group Snapshot copy of all the storage devices in the ASM file system.

SnapManager also provides fast and efficient restores for ASM-based databases. In an ASM configuration, an ASM disk group can be shared by multiple databases. Therefore, reverting to an older Snapshot copy of the disk group is no longer possible, because it would revert all the databases as well. Traditional restore solutions go through the host and require that all the blocks that constitute the database be moved from the storage system to the host and then back to the storage system. The solution provided by SMO removes this overhead. SnapManager restores only the required data within the ASM disk group, without going through the host for most scenarios.
SnapManager can also create quick and space-efficient clones of ASM databases. SnapManager is aware of the ASM disk header format and can clone an ASM disk group by restamping the LUNs or block devices created on NFS volumes.

**Note:** SnapManager 3.4 for Oracle supports ASM on Linux with and without the use of ASMLib. When ASMLib is not used, udev rules are created in its place to manage device permissions.

### History Maintenance

SnapManager 3.4 for Oracle includes the option of using the GUI or the CLI to maintain the historical operational metadata of critical databases for compliance and auditing requirements in an enterprise. History maintenance is supported for the following database operations:

- Backup create
- Backup verify
- Restore and recovery
- Clone create
- Clone split

History maintenance enables the following configuration options:

- Users can configure history maintenance during the creation of the profile or at any time afterward.
- History can be configured at the individual profile level.
- History information is retained based on the retention specified for each operation. However, users can manually purge the history of the SnapManager operation.
- All operation history is listed in the History tab, or it can be viewed by running the `smo history list` command in the CLI. Users can filter the operation history based on profile or operations.

### 2.2 SnapManager for Oracle Architecture

Figure 1 illustrates the SMO architecture and the components that work together to provide a comprehensive and powerful backup, recovery, and cloning solution for Oracle Databases.
Components

The following components work with the SMO architecture to provide a solution for Oracle Databases:

- **Target database.** The target Oracle Database to be managed by SnapManager can be configured in a variety of ways (single-instance or RAC, ASM or standard file systems, and other combinations). See the NetApp Interoperability Matrix Tool for details about the supported Oracle Database versions, configurations, host operating systems, and protocols.

- **SnapManager server.** The SMO server must be installed on every host that has a database to be managed by SnapManager. The SMO GUI or CLI is used to manage the host volumes through NetApp SnapDrive® software to perform backups, clones, and restores and to protect these backups to secondary storage. SMO has built-in protection intelligence to recognize the protection relationship between the primary and secondary storage at the Data ONTAP end. SnapRestore operations are also supported and can be performed either from the primary or from the secondary storage.

- **SnapDrive.** SnapDrive for UNIX or Windows must be installed on the target database host before you install SMO. SnapDrive simplifies storage management, reduces operational costs, and improves storage efficiency. SnapDrive functionality includes error-free application storage provisioning, consistent data Snapshot copy creation, rapid data recovery, and the ability to easily manage data with its server-centric approach. See the Interoperability Matrix Tool to select the appropriate SnapDrive platform and version based on the operating system running on the target database host. SnapDrive must be installed on every host that has a database to be managed by SnapManager.

- **SnapManager repository.** SnapManager organizes information into profiles. A profile holds information about the database to be managed, including its credentials, backups, and clones. The repository holds data about the operations performed on the profiles. A single repository can hold information on multiple profiles. The repository resides in an Oracle Database. The repository cannot reside in the database that is being backed up by SnapManager. Therefore, at least two databases...
(the SnapManager repository database and the target database that is being managed by SnapManager) must be up and running before you execute SMO.

- **Primary storage system.** The target database uses multiple volumes created on the primary NetApp storage system for laying out its data files, control files, archive logs, and so on. Snapshot copy–based backups of the target database created by SnapManager reside on the primary storage system. One of the core components of a NetApp storage system is the clustered Data ONTAP operating system. Clustered Data ONTAP is a highly optimized, scalable, and flexible operating system for unified enterprise data management. SMO supports clustered Data ONTAP versions 8.2.x and 8.3.x and is available on Linux, Solaris, AIX, and Windows. The following licenses must be enabled on the primary storage system:
  - The protocol (FCP, iSCSI, or NFS)
  - SnapRestore
  - FlexClone
  - SnapVault Data ONTAP primary and/or SnapMirror based on the replication policies used (required only if data protection is enabled)

- **Secondary storage system.** If data protection is enabled on a SnapManager profile, then Snapshot copy backups created by SnapManager on the primary storage system are replicated to a secondary NetApp storage system using SnapVault or SnapMirror. This action is based on the protection policy specified in the SnapManager profile. The following licenses must be enabled on the secondary storage system:
  - The protocol (FCP, iSCSI, or NFS)
  - SnapRestore
  - FlexClone (required if using NFS and if cloning is used in FCP/iSCSI environments)
  - SnapVault Data ONTAP primary and/or SnapMirror, based on the replication policies used (required only if data protection is enabled)

- **Oracle Recovery Manager (RMAN).**

Backups created by using SMO can optionally be cataloged with RMAN to preserve the value of RMAN functions, such as block-level restore or tablespace point-in-time recovery. See Appendix B for an example of block-level restore using RMAN and Appendix C for an example of tablespace point-in-time recovery. Cataloging of SnapManager backups with RMAN is optional.

**Note:** RMAN command options for Oracle Database 12c have changed. SnapManager 3.4 for Oracle does not support CDBs and PDBs.

### 2.3 Licenses

Table 1 shows the license requirements and license types.

<table>
<thead>
<tr>
<th>License</th>
<th>Type</th>
<th>Required or Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapManager for Oracle</td>
<td>Host or storage system</td>
<td>On host Required if using host-based license.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On primary Required if using storage-based license.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On secondary Required if using storage-based license and data protection feature.</td>
</tr>
<tr>
<td>SnapDrive for UNIX and/or SnapDrive for Windows</td>
<td>Host or storage system</td>
<td>On host Required if using host-based license.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On primary Required if using storage-based license.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On secondary Required if using storage-based license and data protection feature.</td>
</tr>
<tr>
<td>OnCommand core package</td>
<td>Host</td>
<td>Required for data protection or RBAC feature for 7-Mode and Monitor protection relationships.</td>
</tr>
</tbody>
</table>
### 3 Best Practices and Requirements

#### 3.1 Oracle Database Layout

SnapManager for Oracle (SMO) seamlessly integrates with the latest Oracle Database releases. These releases are 10gR2, 11g R1/R2, and 12c R1 (12.1.0.1). It also integrates with native Oracle technology (such as RAC, RMAN, ASM, and Direct NFS) across FC, FCoE, iSCSI, and NFS protocols.

SnapManager backs up only the following types of files of an Oracle Database:

- Data files
- Control files
- Archive logs

Table 2 shows the file types that are backed up or restored by SMO.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Managed by SMO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle binaries</td>
<td>No</td>
</tr>
<tr>
<td>Data files</td>
<td>Yes</td>
</tr>
<tr>
<td>Temporary data files</td>
<td>No</td>
</tr>
<tr>
<td>Control files</td>
<td>Yes</td>
</tr>
<tr>
<td>Redo logs</td>
<td>No</td>
</tr>
<tr>
<td>Archive logs</td>
<td>Yes</td>
</tr>
</tbody>
</table>
See Appendix A for sample database volume layouts for different Oracle configurations and protocols.

### Best Practices for General Database Layout and Configuration

NetApp recommends the following best practices for general database layout and configuration:

- The best layout for an SMO environment is subject to business needs. The use of separate NetApp FlexVol® volumes for the database binaries, data files, transaction log files, archive log files, and control files is not mandatory. For more information, refer to [TR-3633: Best Practice for Oracle Databases on NetApp Storage](#).
- Do not use the Oracle Database 12c multi-tenant features with SnapManager 3.4 for Oracle. The Oracle Database 12c multi-tenant option (CDB and PDB format) is not supported.
- Include the database system identifier (SID) in the `oratab` file. SnapManager relies on the `oratab` file to determine which Oracle home to use. Ensure that wildcards are not present in the `oratab` file entries.
- Disk groups for the database can be managed by only one volume manager. ASM disks backed by another logical volume manager are not supported.
- Oracle recommends that ASM disks on Linux be placed on a partition. Based on this recommendation, SMO requires the use of a partition.
- Consider the following guidelines for file systems and disk groups to leverage volume-based restores or full disk group restores:
  - Disk groups should contain data files pertaining to only one database.
  - A disk group containing data files cannot contain other types of files. Temporary data files can exist on the same disk group as the regular data files.
- Consider the following guidelines for volume separation to leverage volume-based restores or full disk group restores:
  - Only data files that are relevant to one particular database should be in the volume on the storage system.
  - In the interest of space management, creating a separate volume for temporary data files helps SnapManager for Oracle avoid creating a Snapshot copy of data that does not need to be protected.

Be aware of the following limitations:

- The SnapManager repository is supported on Oracle Express, Standard, Standard ONE, and Enterprise Editions. However, only Oracle Standard, Standard ONE, and Enterprise Editions databases can be managed by SMO.
- SMO uses SQL*Plus during certain operations. In some cases, SnapManager might not correctly parse SQL*Plus messages in a non-English-speaking locale. The workaround forces Oracle commands executed by SMO to use English without affecting any other users on the host. Implement the workaround by performing the following steps:
  a. Add the following lines under the initial comments in `/etc/init.d/smo_server`

```bash
NLS_LANG=American_America
export NLS_LANG
```
  b. Restart the SMO server.
Best Practices for RAC Databases with SnapManager

Consider the following guidelines for using Oracle RAC databases with SMO:

- The SnapManager server must be installed and running on each node in the RAC environment.
- The listener on each node that services an instance of the RAC database must be configured to use the same port number. Also, the listener that services the primary database instance must be started before initiating a backup.
- The password of the database user that SnapManager for Oracle uses (typically SYS) must be the same for all the Oracle instances in a RAC environment.
- Ensure that the spfile/pfile has the parameter `no_recovery_through_resetlogs=true` or, while opening the database using resetlogs, the RAC database clone could fail with the following error: ORA-38856: cannot mark instance UNNAMED_INSTANCE_2 (redo thread 2) as enabled.
- For mission-critical RAC databases, consider configuring two profiles, each referencing a different instance. Doing so enables backups to continue to run when an instance is unavailable and that either profile can be used to perform a recovery.

Best Practices for Using ASM Databases with SnapManager

Consider the following guidelines for using Oracle RAC databases with SMO:

- Ensure that the data files are not in a disk group that includes the ASM spfile. This situation would block volume SnapRestore operations.
- If ASMLib is being used, the `asm_diskstring` parameter of the ASM instance should begin with `ORCL:*`
- Installing ASMLib is not mandatory. SnapManager 3.4 for Oracle also supports backing up databases without using ASMLib or by using ASMLib supplied by Red Hat or SUSE.
- If ASM with multipathing on Linux is used, make sure that `/etc/sysconfig/oracleasm` has the following variables set:

```
ORACLEASM_SCANORDER=’dm’
ORACLEASM_SCANEXCLUDE=’sd’
```

- Use the `SYSASM` system privilege available with 11gR2 instead of `SYSDBA` to administer an Oracle ASM instance. `SYSASM` grants full access to all Oracle ASM disk groups and management functions. With 11gR2, the `SYSDBA` privilege does not permit running administrative commands on an Oracle ASM instance.
- SnapManager supports backing up files that are stored directly on ASM disk groups when the disk group also contains an ACFS volume. SnapManager does not, however, directly support operations on ACFS volumes.
- SnapManager supports backing up and restoring files that are stored directly on ASM disk groups when the disk group also contains Oracle Cluster Registry (OCR) files or voting disk files. However, Oracle strongly recommends having OCR and voting disks on the disk groups that do not contain database files.
- As recommended by Oracle, NetApp requires exactly one partition for each disk that contains the entire disk.

**Note:** A SnapManager error occurs if an attempt is made to back up an ASM disk that has multiple partitions.
• The ASM disk must be aligned to a 4K NetApp WAFL® (Write Anywhere File Layout) file segment. This alignment implies that the device partition on which the ASM disk is created must be 4K-aligned relative to the device itself. It also implies that the multiprotocol type for the LUN must be set accurately for the operating system. For more information about alignment and compression, refer to TR-3633: Best Practices for Oracle Databases on NetApp Storage.

• SnapManager supports ASM on NFS. See the Interoperability Matrix Tool for the required Oracle patches for ASM on NFS.

• For ASM on NFS, make sure that ASM can discover disks imported by SnapManager by setting the ASM_DISKSTRING parameter appropriately.

  Example:
  Consider the following NFS mount point:

  | Storage1:/vol/oradata | /ora/data | nfs |

  ASM on NFS device file 1: /ora/data/hra/disk1

  Provide the connected path from SnapManager to the ASM_DISKSTRING parameter:

  | ASM_DISKSTRING = /ora/data/hra/disk1, /opt/NetApp/smo/mnt/*/disk1 |

  The wildcards in the ASM_DISKSTRING represent the following:
  - The first * matches the name generated by SnapManager for mount point ./ora/data.
  - The second * matches the directory hra within the mount point.

• SnapManager does not support symbolic links on NFS for ASM environments.

• SMO supports ASMLib 2.1.4 and 2.1.7.

• After upgrading from ASMLib 2.1.4 to 2.1.7, the same profiles and backups created with ASMLib 2.1.4 can be used for restores and clones.

• New devices for ASM can be added and old devices can be removed by using the initasmdisks command.

• The device permissions for disks used for ASM tend to change after every reboot. Set the correct device permissions by using the following parameter:

  Oracleasm.support.without.asmlib = True

• udev rules are used in place of non-ASMLib packages. Beginning with RHEL 6.x, Oracle doesn’t provide the ASMLib package from the Oracle Technology Network; instead, it must be downloaded from the RHEL portal. udev rules are set for effective ASM disk management. If the disks are not set up correctly, then there is a chance that the ASM instance will fail to start with a disk permission problem or change in ownership after reboot. There are three ways to have udev that are specific for a single LUN or for all LUNs. These entries should be added in /etc/udev/rules.d with an associated file such as 91-iscsi-rules. Following the changes, you might need to restart the HAS component of Oracle Cluster Ready Services (CRS).

Specific for the LUN (the whole LUN):
ACTION="add|change",
ENV{DM_UUID}="mpath-3600XXXXX", GROUP="asmadmin", OWNER="oracle", MODE="0660"

#1 Specific partition:
ACTION="add|change",ENV{DM_UUID}="part1-mpath-3600XX",GROUP="asmadmin",
OWNER="oracle", MODE="0660"

#2 All disks:
ACTION="add|change", ENV{DM_UUID}="mpath-3600a09*", GROUP="asmadmin", OWNER="oracle",
MODE="0660"

#3 All partitions for all disks:
ACTION="add|change", ENV{DM_UUID}="part1-mpath-3600a09*",GROUP="asmadmin", OWNER="oracle",
MODE="0660"
If you use #1 and #2, add the lines to udev and start_udev. Rescan and check the output for the syntax: multipath -v3.

Best Practices for Using Databases on NFS with SnapManager

NetApp recommends the following best practices for using databases on NFS with SnapManager:

- Mount the file systems by following the best practice recommendations in TR-3633: Best Practices for Oracle Databases on NetApp Storage.
- Export all the volumes that contain Oracle data files, control files, redo logs, and archive logs and the Oracle home with either `anon=0` or `root=<hostname>`. The second option is more secure. SnapManager runs as the root and must be able to access the file systems that contain the Oracle data.
- The use of DNFS has special performance benefits for Oracle RAC on Linux operating systems. The reason is that Linux does not have a method to force direct I/O, which is required with RAC to ensure coherency across the nodes. As a workaround, Linux requires the use of the `actimeo=0` mount option, which causes file data to expire from the operating system cache immediately. This action can cause the side effect of forcing the Linux NFS client to constantly reread attribute data, which adds latency and increases load on the storage controller. Enabling DNFS bypasses the host NFS client and avoids this damage. Multiple customers have reported significant performance improvements on RAC clusters and significant decreases on Data ONTAP load (especially with respect to other IOPS) when DNFS is enabled.

Note:  NetApp recommends not using symbolic links to the location of the database data files if they are linked from local storage to NFS. SnapManager supports symbolic links only at the mount point level.

- Ensure that the NFS mount options are correct. For more information, refer to TR-3633: Best Practices for Oracle Databases on NetApp Storage. The mount option recommendations are subject to change.

3.2 SnapManager Repository Layout

SMO uses a repository to store metadata for the databases that it manages. This repository must reside in an Oracle Database. Part of the installation process of SMO involves creating the repository in a schema of a previously created Oracle Database. The repository holds metadata information for the databases and their backups and clones that SnapManager manages, so it’s critical to follow the best practices described here when planning and creating the repository.

Best Practices for Repository Installation and Sizing

Because the SnapManager repository must reside in an Oracle Database, NetApp recommends using a dedicated database. NetApp does not recommend using an existing Oracle Database that is shared with other applications for the following reasons:

- The repository should be on a single-instance database. RAC could be used, but the SnapManager server would not be able to detect an instance failover.
- The Oracle versions and patch levels supported by SMO might be different from those required by other applications.
- Maintenance such as upgrades and patches of other applications affects the availability of the SnapManager repository, which in turn affects SnapManager operations (backups, restores, and cloning) on databases managed by SMO.
- NetApp recommends deploying the databases used for the SnapManager repositories on NetApp storage systems to simplify repository backup.
- The size of the repository determines how many backup records it can hold. NetApp testing shows that the size of a single backup record in the repository is approximately 100KB. At this size, even a
A repository of 100MB can hold approximately 1,000 backup records. A 200MB Oracle Database would amount to 250 backups, for an environment with 8 Oracle Databases each.

- Protecting the SnapManager repository is critical. SMO cannot back up and restore its own repository. In small environments, protecting repository data can be as simple as installing the database in a single Data ONTAP volume without archive logging and scheduling Snapshot copies directly on the storage system.
- For larger environments, NetApp recommends creating at least two repositories. Then cross-backups (that is, repository X has a profile of repository Y and vice versa, as shown in Figure 2) can be performed by using SnapManager. More than two repositories can be created, but managing numerous repositories can be complex. The total number of repositories depends on the method used to organize the target databases into the repositories.

**Figure 2) Example layout of a SnapManager for Oracle repository.**

Target database profiles can be organized among the SnapManager repositories in many ways. For example, in an environment with different distinct applications, such as customer relationship management (CRM) and human resources (HR), then a SnapManager repository could be created for each application type. The same SnapManager repository would manage all production, development, and testing databases of that application type to help group similar databases and ease cloning. However, when several application types exist, then several SnapManager repositories must be managed, which could increase management complexity. Another SnapManager repository would need to be created for every additional application type. Furthermore, these SnapManager repositories would include production databases, meaning that the repository would have to be protected and availability would be critical.

A second option would be to distribute the databases among the SnapManager repositories based on their usage (for example, production, development, testing, training, and so on). This option limits the number of repositories to the different types of databases. Because all production databases are managed by a single SnapManager repository, only production database administrators (DBAs) would need access to this repository. Also, if another database is deployed for a new application type, then that database must be registered only in the corresponding SnapManager repository instead of your having to create a new repository.

Another variation of the previous distribution is to distribute all production databases in a single SnapManager repository and all of the other nonproduction databases (for example, development, testing, training, and so on) in a different repository. This variation is shown in Figure 2.
has the same advantage as the previous distribution, with the added benefit of reducing the number of SnapManager repositories to two.

However, managing repositories by usage presents challenges. For example, certain production databases are also used for cloning for test and development purposes, and the administrator might have difficulty in identifying which repository to use. NetApp advises its customers to define and select their own preferred method, which might differ from the ones mentioned in this section.

After two repositories have been created, they cannot be merged into one repository. SnapManager does not support merging two or more repositories. Therefore, define a plan before creating multiple repositories. This section describes the requirements and best practices for configuring and installing SnapManager:

- SnapDrive for UNIX or SnapDrive for Windows and any associated prerequisites must be installed and configured before installing SMO.
- Beginning with SnapManager 3.1 for Oracle, users can perform a rolling upgrade, which enables them to upgrade to a later version of SMO on one or more hosts at a given time. Hosts that are not upgraded continue to manage their target databases with their old repository schemas. As part of the upgrade process, all operations performed using the old SnapManager version are imported into a new repository database schema. This phased upgrade gives users a chance to move to a later version of SMO without bringing down all the database host servers. It is also possible to undo the process to an older repository version when the user wants to do so to an older version of SMO.
- Before executing a rolling upgrade or a rollback, see the rolling upgrade section in SnapManager 3.4 for Oracle Administration Guide.
- The target database SID should be included in the oratab file. SnapManager relies on the oratab file to determine which Oracle home to use. If SnapManager cannot find the SID in the oratab file, the profile verification operation fails.
- NetApp recommends allocating sufficient space for the /opt/NetApp/sm0/tmp directory. SnapManager uses this directory to hold temporary safe copies while it performs an operation.
- NetApp recommends replicating SnapManager backups of all critical databases to a secondary storage system by leveraging the policy-driven data protection feature in version 3.4.
- If SMO has been configured to catalog backups with RMAN, make sure that the retention policy in RMAN does not delete the backup information from its catalog before SnapManager purges the backup.
- If SnapManager will be used instead of RMAN for recovery, NetApp recommends not specifying the RMAN information in the profile. Doing so significantly reduces the time required to back up databases. To remove the RMAN information from existing profiles, use the smo profile update CLI command and create a script to update all of these profiles. To complete this step using the GUI, select all of the profiles and update the properties by using the Multiple Profile Update wizard.

### 3.3 SnapManager Operations

#### Best Practices and Requirements for Backup

NetApp recommends the following best practices for backups:

- Perform a full backup of the database to minimize the number of Snapshot copies that SnapManager creates.
  - For details, see “What Full and Partial Backups Are” in the SnapManager 3.4 for Oracle Administration Guide.
- Copy SnapManager backups of all critical databases to a secondary storage system.
- Free backups on primary storage only after they are copied to secondary storage.
- SnapManager can be configured to catalog database backups with RMAN. When using an RMAN recovery catalog, locate it in a database other than the database that is being backed up.
- Include the target database SID in the `oratab` file. SnapManager relies on the `oratab` file to determine which Oracle home to use.
- Start the listener for RAC databases that services the primary database instance before initiating a backup.
- Use the built-in scheduler in the SnapManager GUI to schedule backups. This process gives DBAs who use the SnapManager GUI the added benefit of managing backup schedules and backups from the same interface. Also, backup schedules created and modified by one DBA are visible to all other DBAs who use the SnapManager GUI.
- Delete database backups that are no longer in use to free up space. Use the `smo backup delete` command to delete backups created by SnapManager. This step also reduces the probability of reaching the limit of 255 Snapshot copies per volume.
- Delete backups created by SnapManager by using only the SnapManager GUI or CLI. Deleting Snapshot copies created by SnapManager from SnapDrive or Data ONTAP causes inconsistency between the environment and the SnapManager repository.

**Requirements for Using Fast Restore in SnapManager**

Fast restore (also known as volume restore) is the quickest restore mechanism available among all the restore mechanisms that SnapManager offers. DBAs can leverage the fast restore feature to restore a database in a few minutes regardless of the size of the database. This functionality is optional and is not available on Windows.

**Note:** Enhancements in clustered Data ONTAP 8.2 and later reduced the need for the fast restore. It remains the fastest method of restoration. However, in many cases the new capability to restore individual files or LUNs directly from a Snapshot copy is just as fast and has fewer restrictions on overall configuration. For further details, see TR-3633.

Performing a fast restore can have the following negative consequences; use it with caution.

- The entire storage-side volume is restored, including:
  - Files that were not considered part of the backup
  - Other files, file systems, or LUNs in the volume
- All Snapshot copies that were taken after the Snapshot copy to which the volume is being restored are deleted. For example, Tuesday's backup cannot be restored if Monday's backup was fast restored.
- Relationships to secondary storage systems are broken if the restored Snapshot copy is older than the baseline Snapshot copy in the relationship.
- Volume restore cannot be used when restoring from secondary storage systems.

For details on other file-based restore methods performed by SnapManager, see “What Database Restore Is” in the *SnapManager 3.4 for Oracle Administration Guide*.

When a backup is fast restored, SnapManager first performs mandatory checks and eligibility checks that you can override to determine whether it can use the fast restore process. SnapManager conducts fast restores only on data files. To fast restore backups of a database, consider the following guidelines while planning the database layout:

- For file systems and disk groups:
  - Multiple databases cannot share the same disk group.
  - A disk group that contains data files cannot contain other types of files. Temporary data files can exist on the same disk group as the regular data files.
  - The LUNs for the data file disk group must be the only objects in the storage volume.
- For volume separation:
  - Data files for only one database must be in the volume.
Although SnapManager can fast restore the data files volume even if it contains temporary data files, NetApp recommends creating a separate volume for temporary data files. That is because SnapManager does not back up these files. Including the temporary data files in the same volume as the data files increases the size of the Snapshot copies of that volume.

SMO provides a preview and an analysis option for a fast restore operation before it takes place. The preview section describes how each file in the database will be restored. The analysis section presents the reasons why more efficient restore mechanisms will not be used.

**Recommendations for Freeing Backups and Deleting Backups**

Table 3 explains the differences between freeing and deleting a backup.

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Freeing Backups</th>
<th>Deleting Backups</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI navigation</td>
<td>Right-click Backup and select Free.</td>
<td>Right-click Backup and select Delete.</td>
</tr>
<tr>
<td>CLI execution</td>
<td>smo backup free.</td>
<td>smo backup delete.</td>
</tr>
</tbody>
</table>

- **Are the associated Snapshot copies deleted?**
  - If backup is not protected: Yes.
  - If backup is protected: Yes on primary but retains the protected Snapshot copies on secondary.
  - If a mirror relationship is used, then Snapshot copies are deleted on the primary node. Also, the protected Snapshot copies are deleted from the mirror nodes when the transfer to the secondary node occurs.
  - If backup is protected: Yes (on primary and secondary).

- **Does it free up space occupied by the associated Snapshot copies?**
  - Yes.
  - Yes.

- **Is the backup record retained in the repository after the operation?**
  - Yes.
  - No.

- **After performing this operation on a backup, can the database be restored from the backup by using SnapManager?**
  - Yes, provided that a backup exists on the secondary or a copy of a backup exists in an alternate location.
  - No.

- **When should this option be used?**
  - Use after copying a backup to a secondary location by using scripts that leverage SnapVault or SnapMirror or by any other means. For protected backups, SnapManager automatically frees the backups on primary locations based on the backup retention policy specified in SnapManager.
  - Use when the backup will never be used again.

**Restore from Alternate Location**

SMO cannot integrate with the Protection Manager module of the OnCommand Unified Manager when used with clustered Data ONTAP. Instead, it provides a built-in solution that leverages SnapVault and SnapMirror technology to copy the SnapManager backups from primary to secondary storage. However, for 7-Mode you must still use OnCommand Unified Manager for protection of backups.
To restore from an alternate location, first create a restore specification XML file that specifies the mappings required by SnapManager to restore from the alternate location and to the original location. The original location is the location of the file on the active file system at the time of the backup. The alternate location is the location from which a file will be restored. For details on how to restore from an alternate location, see “Restoring Backups from an Alternate Location” in the SnapManager 3.4 for Oracle Administration Guide.

To restore and recover a backup from an alternate location, complete the following steps:

1. Evaluate your database layout and determine what must be restored:
   a. Restore the required data files from tape, SnapVault, SnapMirror, or any other media to any file system mounted on the database host.
   b. Restore the required file system and mount it on the database host.
   c. Connect to the required raw devices that exist in the local host.
2. Create the restore spec XML file with the original and alternate location mappings, and save the file in a location that is accessible from the SnapManager GUI or CLI.
3. Use the SnapManager GUI or CLI to restore and recover the backup, and specify the location of the restore spec XML file.
4. In the SnapManager Restore and Recovery wizard, select the Use Alternative Restore Specification option to specify the location of the restore spec XML file. See section 6.1, “Disaster Recovery,” for information about how to use this feature to provide a scripted disaster recovery (DR) solution.

Recommendations for Handling Archive Log Files

SnapManager 3.4 for Oracle supports pruning of archive log destinations after taking archive log backups:

- Users can prune the archive logs from single or multiple archive log destinations, along with full, partial, or archive-only backups.
- The scope for pruning can be until a system change number (SCN) occurs, until a specified time period occurs, before a specified time period, or for all logs.
- SnapManager prunes only the archive logs that are backed up, shipped to a standby database in an Oracle Dataguard configuration or captured by Oracle streams.
- SnapManager does not support pruning archive logs from flash recovery areas or standby databases.
- NetApp does not recommend using both RMAN and SMO to manage archive logs.

Consider the following items when making a backup:

- Archive log backups taken along with data file backups are retained based on the retention specified for data file backups during profile creation. That is when the duration of the archive log backup is less than the duration of the data files backup.
- When archive log backup is selected, users can choose single or multiple destinations to be backed up, pruned, or excluded.
- If any archive log files are on a third-party storage system, then the SnapManager operations will fail. The exclude parameters in the smo.config file exclude archive logs on these locations while performing SnapManager operations. For more information, see “List of Configuration Parameters” in the SnapManager 3.4 for Oracle Administration Guide.
- After each archive log backup, SMO consolidates the archive log backups by freeing them with duplicate archive log files and retaining only the archive log backups that have unique archive log files. The archive log consolidation is controlled by the archivelogs.consolidate parameter in the smo.config file.
- Data ONTAP limits the maximum number of Snapshot copies to 255 per volume. This maximum number might be reached if SnapManager is configured to retain a large number of backups in which
each backup consists of numerous Snapshot copies. Configure appropriate retention policies to remove successful backups after reaching a specific threshold for a specific backup retention class.

- For RAC configurations, SMO performs the backup on the host that is specified in the SnapManager profile. SMO backups taken from one node of a RAC cannot be restored on any other nodes of the cluster. If the RAC host is down, the backup fails. Similarly, if the node is down during a restore, the restore fails.

**Restore and Recover RAC Databases**

SnapManager for Oracle can be invoked from any RAC database node to restore and recover. The RAC node where SnapManager performs the restore and recovery operation does not need to be the same as the node where the backup was performed.

Note the following recommendations for recovering a RAC database:

- Ensure that all of the archive log files are available in the backups or in one external archive log destination.
- When pruning the archive log files, don’t delete all of them manually. Instead, delete the archive log files until SCN or until a specified date so that the backups can overlap the archive log files.
- NetApp recommends using the Restore Preview option to analyze the effect of the fast restore operation before executing it.

If a database control file is being used as the RMAN repository, instead of having a separate database for RMAN, be careful when restoring the control files. Users will lose all backup information cataloged in the control file taken after the backup of a control file is restored.

- To restore ASM databases by using the new SnapManager Restore feature from an alternate location when restoring files on a mounted file system, the ASM disk group name must be the same as the disk group name that SnapManager cloned to register the backup with RMAN. This name can be viewed in the Backup Properties page.

**Cloning Databases**

**Cloning Technologies**

In UNIX-based environments, SMO leverages FlexClone technology when cloning in NFS. However, SMO can optionally leverage FlexClone technology or LUN-clone technology in SAN environments.

Table 4 describes the possible values that can be specified for the `san-clone-method` option in the `snapdrive.conf` file.

<table>
<thead>
<tr>
<th>Snapdrive.conf Variables and Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>san-clone-method=lunclone</code></td>
<td>Only creates a LUN clone.</td>
</tr>
<tr>
<td><code>san-clone-method=unrestricted</code></td>
<td>Creates a FlexClone volume that can be used as a back end for provisioning and Snapshot operations, similar to normal flexible volumes.</td>
</tr>
<tr>
<td><code>san-clone-method=optimal</code></td>
<td>SnapDrive attempts to create a FlexClone volume. If it cannot, it reverts to the LUN-clone method.</td>
</tr>
</tbody>
</table>

SnapDrive for UNIX 5.2.x and later checks the following items to verify that it can create a FlexClone volume:

- The storage system Data ONTAP version is 7.3.2 or later and the FlexClone technology is licensed.
- The host `filespec` residing volume is a flexible volume.
A host filespec can be a file system, host volume, disk group, or LUN.

The host filespec residing volume is not the storage root volume.

Adequate space is available on the aggregate.

If any of the preceding checks fails, SnapDrive for UNIX performs the following actions:

- Errors out for an unrestricted FlexClone volume
- Falls back to the lunclone method for a FlexClone volume (if the clone method is Optimal)

For the changes to take effect, the SnapDrive daemon must be restarted after each modification to the snapdrive.conf file.

Apply the following best practices when cloning databases:

- Although a separate license is not required for creating LUN clones, license FlexClone even in SAN environments and configure SnapDrive accordingly, if required. Doing so enables SnapManager to leverage FlexClone technology while cloning in both NFS and SAN environments.
- Oracle Database 11g in a direct NFS environment allows additional mount point configurations, such as multiple paths for load balancing, in the oranfstab file. SnapManager does not modify this file; therefore, manually add any additional properties that the clone requires to the oranfstab file after cloning with SnapManager.
- Assign a new Oracle SID to the clone. Oracle does not allow two databases with the same SID to run simultaneously on the same host. A clone on a different host can use the same SID. In that case, a new label option designates a unique name for the clone. If this option is not used, SnapManager creates a unique name for the clone that includes the SID, date, and time.
- When using TNSNAMES, add the details of the newly created cloned database to the TNSNAMES file on the client machines that must access this database.

Clone RAC Databases

SMO clones a RAC database to a non-RAC database and sets the Oracle parameter cluster.database to False. The parameter can then be changed to a RAC database manually. For steps on how to perform this conversion, see Appendix D.

Note: Cloning the online database backup of the RAC database by using the external archive log file location fails because of a failure in recovery. Oracle fails to find and apply the archive log files for recovery from the external archive log location while cloning the database backup.

Clone on Alternate Host

Review the prerequisites in Table 5 before cloning a database on an alternate host.

Table 5) Prerequisites for cloning a database on an alternate host.

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Requirement on Source and Target Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Must be the same for both the source and target hosts.</td>
</tr>
<tr>
<td>Operating system and version</td>
<td>Must be the same for both the source and target hosts.</td>
</tr>
<tr>
<td>SMO</td>
<td>Must be running on both hosts.</td>
</tr>
<tr>
<td>Credentials</td>
<td>An Oracle user's group ID should be the same on the source and the target host.</td>
</tr>
<tr>
<td>Oracle</td>
<td>The same software must be installed. An Oracle listener must be running on the target host.</td>
</tr>
<tr>
<td>Compatible storage stack</td>
<td>Must be the same for both source and target hosts.</td>
</tr>
<tr>
<td>Protocol used to access data files</td>
<td>Must be the same for both source and target hosts.</td>
</tr>
</tbody>
</table>
Before cloning an ASM database on an alternate host, verify the following:

- An ASM instance is running on the target host.
- The ASMLib version is the same as it is on the primary host.

**Clone Other Clones**

SnapManager currently does not automatically create a new profile for database clones. To back up and clone a clone database, create a new profile for the clone database in SMO. After this step is completed, regular SnapManager operations such as backing up and cloning the clone database can be executed.

For example, complete these steps to upgrade a production database:

1. Create a SnapManager profile for the production database.
2. Back up the production database before upgrading.
3. Create a clone for development by using the preupgrade production database backup.
4. Create a SnapManager profile for the development database (clone of production).
5. Upgrade and back up the development database.
6. Create a clone for QA by using the upgraded development database.
7. Create a SnapManager profile for the QA database (clone of development after upgrade).
8. Back up the QA database.
9. Create a clone for regression testing by using the QA database backup.
10. Create another clone for load testing by using the QA database backup.

Figure 3 shows how to manage various clones in SnapManager for Oracle.
**Splitting Clones**

Clone splitting is supported only for FlexClone volumes, not for lunclones. This feature is not supported on Windows.

Users should consider splitting a clone in the following scenarios:

- To free Snapshot copies associated with the clone so that they can be deleted
- To retain the clone longer without having to retain the parent backup
- If many block changes in the clone affect performance in the caching algorithm

When a clone is split successfully, SnapManager creates a new profile for the clone. Users can create database backups, restore data, and create clones by using this new profile.

SnapManager also performs clone splitting estimates. These help determine the total free space available on the aggregate, the amount of space shared between the clone and the original database, and the space extensively used by the clone. DBAs should evaluate this data to decide whether or not to split a clone.

**Deleting Clones**

Business requirements determine how long a clone database should be retained or cloned again from a new backup. Deleting and cloning from a new backup prevent the clones from using too many resources and make sure that the clone has the most current data for testing or development.

### 3.4 Event Logging

The SnapManager server logs are stored under:
SnapManager manages the server log files automatically, based on user-defined values of the following parameters in the SnapManager configuration file, smo.config:

- `log.max_log_files`
- `log.max_log_file_size`
- `log.max_rolling_operation_factory_logs`

Therefore, the directory in which the server logs are written will not exceed the limit. The SnapManager configuration file, smo.config, is located under the properties directory in the directory in which SnapManager is installed. For example, in Linux, the path of the file is:

```
/var/log/smo
```

SnapManager 3.4 for Oracle enables the user to control the level of logs generated. This is helpful for controlling the messages being logged by SnapManager. For example, the log level can be changed to `DEBUG`, which logs additional messages and can assist in debugging some operational issues.

To override the default level, complete the following steps:

1. Create a `platform.override` text file in the SnapManager installation directory.
2. Add a `server.log.level` key in the `platform.override` text file.
3. Assign one of these level values (`TRACE`, `DEBUG`, `INFO`, `WARN`, `ERROR`, `FATAL`, `PROGRESS`) to the `server.log.level` key.
   - Example: `server.log.level=ERROR`
4. Restart the SnapManager server.

### 3.5 NetApp Recommendations for Upgrading Oracle Database with SnapManager

Upgrading databases with less downtime and space, and more reliability is a key capability of SnapManager for Oracle. Enterprises can take instant copies of production databases and upgrade them to use as development or testing databases with limited resources, unlike with the traditional method. The SnapManager upgrade method helps to retain a database production copy and makes it easy to restore it within a few minutes in the event the upgrade process fails.

- Design volume and LUN layouts according to Oracle best practices. Make sure that you have sufficient space in the volume or aggregate if it needs split operations.
- You must meet all SnapManager installation and configuration prerequisites, such as host utilities and SnapDrive installed for UNIX, on both source and target servers.
- Make sure that the version of Oracle is the same on the source and target servers.
- Create a FlexClone volume of the source database to the alternate host having the same source Oracle home.
- Upgrade to the target version using `catupgrade` or the `dbupg` tool. Refer to the upgrade procedure from the Oracle Technology Network.
- The time that it takes to split a clone depends on the volume of data. Splitting a clone makes it independent from the parent volume.

### 3.6 Recommendations for Enabling Data Protection

SnapManager 3.4 natively supports data protection for clustered Data ONTAP systems, whereas systems running Data ONTAP operating in 7-Mode still use OnCommand Unified Manager for protection. The
Mirroring relationships should be carefully chosen, understanding the purpose and requirements of the application. For long retention of backups, SnapVault can be used to protect backups from primary to secondary, with the limitation of 251 Snapshot copies for each volume. SnapMirror is used for mirroring the volumes by replicating them to the same level of source volume by copying all of the Snapshot copies periodically.

Proper cluster or Vserver peering is required for data protection. Such peering tries to allocate space from the aggregate while creating mirror or vault volumes. To establish mirror or vault volumes across different storage volumes, use cluster peering. Through this peering, intercluster LIFs are created on both nodes and are exchanged with a passphrase, as shown in Figure 4 and Figure 5.

Figure 4) Intercluster peering.

![Intercluster peering](image)

Figure 5) Protection relationship state.

![Protection relationship state](image)

Make sure that the protection policy is created with a SnapVault label and with the desired retention count on the Data ONTAP storage. The secondary volumes cannot retain more than 251 Snapshot copies, whereas the primary can retain 255. The protection state should be shown as healthy and the relationship state as SnapMirrored.

Schedule the Data ONTAP Snapshot copy policies carefully by choosing different labels and intervals so that they don’t hinder the SnapMirror update operation of SMO.

Each backup from SMO should carry an appropriate SnapVault label that was already configured from the storage end. Having these labels will make sure that the Snapshot copies are replicated to secondary storage by matching those labels.
# Sample Setup

## 4.1 SMO Configuration, Backup, Clone and Restore

Table 6 shows steps to configure SnapManager and to create a profile with protection.

<table>
<thead>
<tr>
<th>Prerequisite Tasks</th>
<th>Example Tasks</th>
</tr>
</thead>
</table>
| Verify that all the prerequisites described in the [SnapManager 3.4 for Oracle Installation and Administration Guide](#) have been met. | • Check the NetApp [Interoperability Matrix Tool](#) to verify that all of the components in your environment are supported.  
• Verify that all required licenses are enabled. |

<table>
<thead>
<tr>
<th>Repository Host Setup</th>
<th>Example Commands</th>
</tr>
</thead>
</table>
| Identify an existing Oracle Database and listener port for the SnapManager repository. | • Identify the Oracle SID of the database and verify that the database is open:  
  # su - oracle  
  [oracle@repo_host1~]# cat /etc/oratab  
  • Identify the Oracle listener port for this database and verify that the listener port has been started:  
  [oracle@repo_host1~]$ LSNRCTL> status |
| Create a tablespace to be used by the SnapManager repository in the preceding database. | • Create a new tablespace for the SnapManager repository:  
  SQL> create tablespace smo datafile '/u01/oradata/datafile/smo01.dbf' size 100M autoextend on maxsize 1000M;  
  • SnapManager requires a minimum 4K block size for the tablespace into which it is installed. Check the block size for the smo tablespace by using the following command:  
  SQL> select tablespace_name, block_size from dba_tablespaces where tablespaces_name = 'SMO';TABLESPACE_NAME BLOCK_SIZE  
  -------------------------------  ----------  
  SMO 8192  
  Create an Oracle user who will own the SnapManager repository in the preceding database. | SQL> create user smoadmin identified by adminpw1 temporary tablespace temp default tablespace smo quota unlimited on smo; |
| Only grant connect and resource roles to the preceding database user. | SQL> grant connect, resource to smoadmin |

Target Database Host Setup

Install, configure, and verify SnapDrive on

Download the appropriate SnapDrive software file for your host platform from the NetApp Support site.
| all the target database hosts. | - SnapDrive should be installed on every host that has one or more databases that will be managed by SnapManager.  
- Log in as root and install the SnapDrive software.  
- SnapDrive for UNIX defaults to use the https connection. To make SnapDrive for UNIX use the http protocol to communicate to the storage system, edit the snapdrive.conf file and set it to use-https-to-filer=off.  
- Restart the SnapDrive daemon every time you modify the snapdrive.conf file to have the changes take effect:  
  ```
  [root@tardb_host1 snapdrive]# snapdrived restart
  ```  
- Configure SnapDrive and specify which operating system user will be used to access the NetApp storage system used by the target databases:  
  ```
  [root@tardb_host1 snapdrive]# snapdrive config set root my_netapp_storage_system1
  ```  
- Verify that the configuration was successful:  
  ```
  [root@tardb_host1 snapdrive]# snapdrive config list
  user name          filer name
  -------------------------
  root                my_netapp_storage_system1
  ```  |
| Install the SMO software on all the target database hosts. | - Download the appropriate SnapManager 3.4 for Oracle software file for your host platform from the NetApp Support site.  
- SnapManager software should be installed on every host that has one or more databases that will be managed by SnapManager.  
- Log in as root and install the SMO software.  
- SnapManager software should be installed on all the hosts of a RAC database.  
| Start the SnapManager server on the target database host. | - Note the port number on which the server is started. This port is used to launch the SnapManager GUI from a web browser. The default port is 27214. |
| Verify that the SnapManager installation was successful. | - SQL> create user smo_oper identified by operpw1;  
- To manage a database, SnapManager requires that an Oracle user with the sysdba role connect to that database and perform database operations:  
  ```
  SQL> grant sysdba to smo_operator;
  ```  
| Create an Oracle user with the sysdba role for the target database that will be managed by SMO. | Note: If using the database-authentication connection mode, either use an existing database user with the sysdba role (such as sys) or create a new database user and grant the sysdba role. |
| To register SnapManager backups with RMAN, SnapManager requires registering the target database with RMAN. | - SQL> create user smo_oper identified by operpw1;  
- To manage a database, SnapManager requires that an Oracle user with the sysdba role connect to that database and perform database operations:  
  ```
  SQL> grant sysdba to smo_operator;
  ```  
- Note: If using the database-authentication connection mode, either use an existing database user with the sysdba role (such as sys) or create a new database user and grant the sysdba role. |
| Install the SMO software on all the target database hosts. | - Download the appropriate SnapManager 3.4 for Oracle software file for your host platform from the NetApp Support site.  
- SnapManager software should be installed on every host that has one or more databases that will be managed by SnapManager.  
- Log in as root and install the SMO software.  
- SnapManager software should be installed on all the hosts of a RAC database.  
| Start the SnapManager server on the target database host. | - Note the port number on which the server is started. This port is used to launch the SnapManager GUI from a web browser. The default port is 27214. |
| Verify that the SnapManager installation was successful. | - SQL> create user smo_oper identified by operpw1;  
- To manage a database, SnapManager requires that an Oracle user with the sysdba role connect to that database and perform database operations:  
  ```
  SQL> grant sysdba to smo_operator;
  ```  
| Create an Oracle user with the sysdba role for the target database that will be managed by SMO. | Note: If using the database-authentication connection mode, either use an existing database user with the sysdba role (such as sys) or create a new database user and grant the sysdba role. |
| To register SnapManager backups with RMAN, SnapManager requires registering the target database with RMAN. | - SQL> create user smo_oper identified by operpw1;  
- To manage a database, SnapManager requires that an Oracle user with the sysdba role connect to that database and perform database operations:  
  ```
  SQL> grant sysdba to smo_operator;
  ```  
<p>| Create an Oracle user with the sysdba role for the target database that will be managed by SMO. | Note: If using the database-authentication connection mode, either use an existing database user with the sysdba role (such as sys) or create a new database user and grant the sysdba role. |</p>
<table>
<thead>
<tr>
<th>Launch SnapManager GUI or CLI</th>
<th>Example Commands</th>
</tr>
</thead>
</table>
| CLI                           | • The SnapManager CLI can be accessed from any host where the SnapManager server has been installed.  
• Any target database host can be used to access the SnapManager CLI on which SnapManager software is already installed. Alternatively, use a dedicated host to issue only the SnapManager commands through the CLI. The SnapManager software still must be installed on this dedicated host to access the CLI.  
• All SnapManager commands start with smo. |
| GUI                           | The SnapManager GUI launches from a web browser on any host running an operating system supported by SMO:  
https:// smo-server . domain . com : port  
• smo - server is the name of the host in which the SnapManager server was installed and started.  
• domain . com is the domain of the SnapManager server host.  
• port is the port number on which the SnapManager server was started; the default port number is 27214. |

<table>
<thead>
<tr>
<th>Credentials, Repository, and Profiles Setup</th>
<th>Example Commands</th>
</tr>
</thead>
</table>
| **Set repository access credentials for every operating system user who will use SnapManager.** | 1. Log in as the operating system user:  
`smo credential set -repository -host repo_host1 -dbname smorepo -port 1524 -log in -username smoadmin`  
2. Enter a password for database connection:  
`smoadmin@repo_host1:1524/smorepo:**********`  
3. Execute the preceding command for all target database hosts that this operating system user will access by using SnapManager. |
| **Create the SnapManager repository by using SnapManager.** | SMO GUI  
Operations > Repository > Create New Repository  

**SMO CLI**  
`somo repository create -repository -dbname smorepo -host repo_host1 -port 1524 -log in -username smoadmin` |
Profile created with protection enablement and validation.

SMO GUI

Operations > Repository > Create Profile

Profile Configuration Information

- Profile Name: [SNMPROD]
- Password: [***********]
- Confirm Password: [***********]
- Comment: [Optional for the profile]

Database Configuration Information

- Database Name: [PROD]
- Database SID: [PROD1]
- Host: [10.72.199.89]

Help < Back Next > Cancel
Profile created with green check icon across it to show it conforms or that protection is enabled.

### SMO GUI

![SMO GUI](Image)

### SMO CLI

- **Without RMAN, not protected:**
  
  ```bash
  smo profile create -profile targetdb1_prof1 -profile-password tardbpw1 -repository -dbname smorepo -log in -username smoadmin -host repo_host1 -port 1524 -database -dbname tardbl -logIn -username smo_oper -password operpw1 -host tardb_host1 -port 1521 -sid tardbl -osaccount oracle -osgroup dba -retain 100 -verbose
  ```

- **With RMAN:**
  
  ```bash
  smorepo -login -username smoadmin -host repo_host1 -port 1524 -database -dbname tardbl -host tardb_host1 -log in -username smo_oper -password operpw1 -port 1521 -sid tardbl -osaccount oracle -osgroup dba -rman -login -username rmanadmin -password rmanpw1 -tnsname rmanrepo -retain 100 -verbose
  ```

## Backup and Cloning Operation with Protection

Backups are similar to previous versions except for protection enablement. A new field for the SnapVault label and clone from the secondary option will be displayed while cloning, as shown in Table 7.

Table 7) Backup and cloning operation with protection.

<table>
<thead>
<tr>
<th>Prerequisite Tasks</th>
<th>Example Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that all the prerequisites described in the SnapManager 3.4 for Oracle Installation and Administration Guide have been met.</td>
<td></td>
</tr>
</tbody>
</table>

- Check the NetApp Interoperability Matrix Tool to verify that all of the components in your environment are supported.
- Verify that all required licenses are enabled.
Repository Host Setup

Create backup with SnapVault label

Click the option

Protect the Backup to enable backup protection. Click Next in further sections to create the backup.

Check if the protection status shows as Protected following the backup process.
Cloning operation:
Provide details for the new test instance that should be cloned from the production/source database. DBAs can select this clone from primary or secondary storage.

Click Environment to add new SID-relevant details. Click Next to start the clone.

Restore and Recover Scenarios

Scenario 1: Restore Whole Database Without Control Files and Recover All Available Logs

In this scenario, the current control files exist, but all the data files are damaged or lost. Restore and recover the database from an existing full online backup using all available logs.

Using the GUI

To restore the database by using the GUI, complete the following steps:

1. Right-click Backup and select Restore/Recover to launch the Restore and Recovery wizard.
2. In the Restore Configuration Information page of the wizard, select the Complete Datafile/Tablespace Restore Without Control Files option. Click Next.

3. In the Recovery Configuration Information page of the wizard, select All Logs. Click Next.

4. Proceed through the remaining pages of the wizard.

Using the CLI

To restore the database by using the CLI, run the following command:

```
smo backup restore -profile targetdb1_prof1 -label full_bkup_sales_apr_12 -complete - recover -alllogs -verbose
```

Workflow Example

```
SQL> select * from company;
     ID  COMPANY_NAME
----------  -------------------
     1     NETAPP

[root@node3 ~]# cd /mnt/nfs1/oradata/hra/
[root@node3 hra]# ls
example01.dbf  sysaux01.dbf  system01.dbf  temp01.dbf  test01.dbf  undotbs01.dbf  users01.dbf
[root@node3 hra]# rm -rf *

SQL> startup;
ORACLE instance started.

Total System Global Area 1002127360 bytes
   Fixed Size                  2165888 bytes
   Variable Size             679478144 bytes
   Database Buffers          314572800 bytes
   Redo Buffers                5910528 bytes
Database mounted.

ORA-01157: cannot identify/lock datafile 1 - see DBWR trace file
ORA-01110: datafile 1: '/mnt/nfs1/oradata/hra/system01.dbf'
```
Below is a summary of your operation configuration.

Restore the backup of database "hra" in profile "HRA_RMAN".

Restore Configuration Information
  Restore Control File(s): No
  Restore Datafile(s) or Tablespace(s): Yes

Restore Scope: Complete
  Allow shutdown of database if necessary: No

Recovery Configuration Information
  Recovery to Perform: All Logs
  Use Backup Control Files: No

Restore Source Location:
  Use local storage for the restore

Volume Restore Configuration Information:
  Perform volume restore, falling back to traditional restore, if necessary

Task Specification:
  Pre Task(s):
    Not Enabled
Scenario 2: Restore Whole Database Without Control Files and Recover to Particular SCN

In this scenario, the current control files exist, but all the data files are damaged or lost or a logical error occurred after a particular SCN.

Using the GUI

To restore the database by using the GUI, complete the following steps:

1. Right-click Backup and select Restore/Recover to launch the Restore and Recovery wizard.
2. In the Restore Configuration Information page of the wizard, select the Complete Datafile/Tablespace Restore Without Control Files option. Click Next.
3. In the Recovery Configuration Information page of the wizard, select SCN and specify the SCN number (2811715) in the text box. Click Next.
4. Proceed through the remaining pages of the wizard.
Using the CLI

To restore the database by using the CLI, run the following command:

```
 smo backup restore -profile targetdb1_prof1 -label full_bkup_sales_apr_12 -complete -recover -until 2811715 -verbose
```

Workflow Example

```
SQL> select current_scn from v$database;
CURRENT_SCN
-----------
2811675

SQL> insert into company select * from company;
2 rows created.
SQL> commit;
Commit complete.

SQL> select count(*) from company;
COUNT(*)
--------
4

SQL> select current_scn from v$database;
CURRENT_SCN
-----------
2811715

SQL> drop table company;
Table dropped.
SQL> commit;
Commit complete.

SQL> select current_scn from v$database;
CURRENT_SCN
-----------
2811770

Restore to SCN 2811715:
```
Below is a summary of your operation configuration.

- Restore the backup of database 'hra' in profile 'HRA_RMAN'.
- Restore Configuration Information:
  - Restore Control File(s): No
  - Restore Datafile(s) or Tablespace(s): Yes
- Restore Scope: Complete
  - Allow shutdown of database if necessary: No
- Recovery Configuration Information:
  - Recovery to Perform SCN: Recover to: 2811715
  - Use Backup Control Files: No
- Restore Source Location:
  - Use local storage for the restore
- Volume Restore Configuration Information:
  - Perform volume restore, falling back to traditional restore, if necessary
- Task Specification:
  - Pre Task(s):

---

Log Messages:

- [INFO] SM0-03066: Recovery succeeded
- [INFO] SM0-03065: End of Database Recovery
- [INFO] SM0-20000: Changing state for database instance 'hra' from MOUNTED to OPEN
- [INFO] SM0-0032: Opening database hra with RESELOGS option
- [INFO] ORACLE-00114: Issuing "RESET DATABASE" command to RMAN.
- [WARN] SM0-02017: External table "SALES_TRANSACTIONS_EXT" in the database was not restored as part of this operation (SnapManager does not backup and restore external tables).
- [INFO] SM0-07131: Unlocked database for SnapManager operation
- [INFO] SM0-07433: Removing the database to its initial state 'hra(OPEN)'
- [INFO] SM0-13048: Backup Restore Operation Status: SUCCESS
- [INFO] SM0-13049: Elapsed Time: 0:02:33.180
- [INFO] Operation Id [8ac847c857bd0b773bd51372b7742db0001] succeeded.

- Log Message Output Level:
  - Fatal
  - Error
  - Warn
  - Info
Scenario 3: Restore Whole Database Without Control Files and Recover Up to Date and Time

In this scenario, the current control files exist, but all the data files are damaged or lost or a logical error occurred after a specific period of time.

Using the GUI

To restore the database by using the GUI, complete the following steps:
1. Right-click Backup and select Restore/Recover to launch the Restore and Recovery wizard.
2. In the Restore Configuration Information page of the wizard, select the Complete Datafile/Tablespace Restore Without Control Files option. Click Next.
3. In the Recovery Configuration Information page of the wizard, select the Date option and specify the date and time in the Date field. Click Next.
4. Proceed through the remaining pages of the wizard.

Using the CLI

To restore the database by using the CLI, run the following command:

```
```

Workflow Example

```
SQL> select current_scn from v$database;
CURRENT_SCN
----------
2813039
SQL> insert into company select * from company;
4 rows created.
SQL> commit;
Commit complete.
SQL> select count(*) from company;
    COUNT(*)
----------
        4
SQL> select current_scn from v$database;
CURRENT_SCN
----------
2813560
SQL> drop table company;
Table dropped.
SQL> commit;
Commit complete.
SQL> select current_scn from v$database;
CURRENT_SCN
----------
2813949
SQL> select scn_to_timestamp(2813560) from dual;
SCN_TO_TIMESTAMP(2813560)
```
SQL> select scn_to_timestamp(2813949) from dual;
SCN_TO_TIMESTAMP(2813949)
05-JUN-12 01.00.14.000000000 PM
SnapManager for Oracle Restore and Recovery Wizard

Recovery Configuration Information

- All Logs
  Recovery to last commit by applying all required logs.

- No Logs
  Recovery to the state at backup and apply no logs.

- Restore Only
  Restore database only, no recovery performed.

- SCN
  Recovery to be performed to selected SCN.

- Date
  Recovery to be performed to selected date.

- Use Backup Control Files

Specify External Archive log Location(s)

To enable edition, click the field once and enter or press F2 key.

NetApp

Completing the SnapManager for Oracle Restore and Recovery Wizard

Point-in-time recovery successful.

NOTE: Warnings occurred during the operation.

See Operation Details for more information.

To close this wizard, click Finish.
Scenario 4: Restore Database Partially (One or More Data Files) Without Control Files and Recover Using All Available Logs

In this scenario, the current control files exist, but one or more data files is damaged or lost.

Using the GUI

To restore the database by using the GUI, complete the following steps:

1. Right-click Backup and select Restore/Recover to launch the Restore and Recovery Wizard.
2. In the Restore Configuration Information page of the wizard, select the Selective Datafile/Tablespace Restore Without Control Files option. Expand the Datafiles list and use the Control key to select one or more data files to be restored. Click Next.
3. In the Recovery Configuration Information page of the wizard, select All Logs.
4. Proceed through the remaining pages of the wizard.

Using the CLI

To restore the database by using the CLI, run the following command:

```bash
smo backup restore -profile targetdb1_prof1 -label full_bkup_sales_apr_12 -files /u02/oradata/sales02.dbf /u02/oradata/sales03.dbf -recovery -alllogs -verbose
```

Workflow Example

```
SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES WHERE TABLESPACE_NAME='USERS';
FILE_NAME                      TABLESPACE_NAME
------------------------------ ------------------------
/mnt/nfs1/oradata/hra/users01.dbf USERS
SQL> select segment_name, tablespace_name from dba_segments where SEGMENT_NAME = 'I30';
SEGMENT_NAME                   TABLESPACE_NAME
------------------------------ ------------------------
I30                            USERS
SQL> insert into i30 select file_id from dba_data_files;
6 rows created.
SQL> select count(*) from i30;
COUNT(*)
-------
6
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
[root@node3 hra]# pwd
/mnt/nfs1/oradata/hra
[root@node3 hra]# rm users01.dbf
rm: remove regular file `users01.dbf'? y
SQL> startup;
ORACLE instance started.
Total System Global Area 1002127360 bytes
Fixed Size                  2165888 bytes
Variable Size              679478144 bytes
Database Buffers           314572800 bytes
```
Redo Buffers 5910528 bytes
Database mounted.

ORA-01157: cannot identify/lock datafile 4 - see DBWR trace file
ORA-01110: datafile 4: '/mnt/nfs1/oradata/hra/users01.dbf'

SnapManager for Oracle Restore and Recovery Wizard

Restore Configuration Information

- Complete Datafile/Tablesce Restore with Control Files
- Complete Datafile/Tablesce Restore without Control Files
- Control Files Restore without Datafiles/Tablesce
- Selective Datafile/Tablesce Restore without Control Files
- Selective Datafile/Tablesce Restore with Control Files

Select either tablespaces or datafiles to restore.

- hra
  - Tablesce
    - Datafiles
      - /mnt/nfs1/oradata/hra/example01.dbf
      - /mnt/nfs1/oradata/hra/sysaux01.dbf
      - /mnt/nfs1/oradata/hra/sys01.dbf
      - /mnt/nfs1/oradata/hra/sysaux01.dbf
      - /mnt/nfs1/oradata/hra/users01.dbf

- Allow shutdown of database if necessary
SnapManager for Oracle Restore and Recovery Wizard

Recovery Configuration Information

- **All Logs**
  - Recovery to last commit by applying all required logs.
- **No Logs**
  - Recovery to the state at backup and apply no logs.
- **Restore Only**
  - Restore database only, no recovery performed.
- **SCN**
  - Recovery to be performed to selected SCN.
- **Date**
  - Recovery to be performed to selected date: 2012-06-06 16:03:33

**Use Backup Control Files**

Specify External Archive log Location(s)

- To enable edition, click the field once and enter or press F2 key.

SnapManager for Oracle Restore and Recovery Wizard

Volume Restore Configuration Information

- **Attempt volume restore**
  - SnapManager will perform a series of checks to ensure volume restore is valid. If all checks pass, a volume restore will occur. However, if any check fails, SnapManager should:
  - **Failback to file-based restore**
  - **Require volume restore and fail the restore if any checks fail**
  - **Override if possible. Perform a volume restore if any overrideable checks fail. Fail the restore if any mandatory checks fail**
  - **Perform file-based restore**
    - File-based restore is required when restoring selected files from a backup
Scenario 5: Restore Only Control Files and Recover Using All Available Logs

In this scenario, the data files exist, but all control files are damaged or lost.

Using the GUI

To restore the database by using the GUI, complete the following steps:

1. Right-click Backup and select Restore/Recover to launch the Restore and Recovery wizard.
2. In the Restore Configuration Information page of the wizard, select the Control Files Restore Without Datafile/Tablespace option. Click Next.
3. In the Recovery Configuration Information page of the wizard, select All Logs.
4. Proceed through the remaining pages of the wizard.

Using the CLI

To restore the database by using the CLI, run the following command:

```
smo backup restore -profile targetdb1_prof1 -label full_bkup_sales_apr_12 -controlfiles -recover -alllogs -verbose
```

Workflow Example
SQL> select count(*) from i30;
COUNT(*)
----------
   48
SQL> commit;
Commit complete.
SQL> alter system switch logfile;
System altered.
SQL> /
System altered.
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.

[root@node3 ~]# cd /mnt/config1/oradata/hra/
[root@node3 hra]# rm control01.ctl
rm: remove regular file 'control01.ctl'? y
[root@node3 hra]# cd /mnt/config2/oradata/hra/
[root@node3 hra]# rm control02.ctl
rm: remove regular file 'control02.ctl'? y
[root@node3 hra]# cd /mnt/config3/oradata/hra/
[root@node3 hra]# rm control03.ctl
rm: remove regular file 'control03.ctl'? y
Scenario 6: Restore Whole Database Without Control Files and Recover Using Backup Control Files and All Available Logs

In this scenario, all data files and control files are damaged or lost.

**Using the GUI**

To restore the database by using the GUI, complete the following steps:

1. Right-click Backup and select Restore/Recover to launch the Restore and Recovery wizard.
2. In the Restore Configuration Information page of the wizard, select the Complete Datafile/Tablespace Restore with Control Files option. Click Next.
3. In the Recovery Configuration Information page of the wizard, select the All Logs and Using Backup Control Files options. Click Next.
4. Proceed through the remaining pages of the wizard.

**Using the CLI**

To restore the database by using the CLI, run the following command:

```
smo backup restore -profile targetdb1_prof1 -label full_bkup_sales_apr_12 -complete -using-backup-controlfile -recover -alllogs -verbose
```

**Workflow Example**

```
SQL> select count(*) from company;
   
   COUNT(*)
----------
       32

SQL> commit;
Commit complete.

SQL> shutdown immediate;

```

```
[root@node3 ~]# cd /mnt/nfs1/oradata/hra
[root@node3 hra]# ls
example01.dbf  i2e1.dbf  sysaux01.dbf  system01.dbf  test01.dbf  test02.dbf  undotbs01.dbf
users01.dbf

[root@node3 hra]# rm -Rf *
[root@node3 hra]# rm /mnt/config1/oradata/hra/control01.ctl
```
rm: remove regular file '/mnt/config1/oradata/hra/control01.ctl'? y
[root@node3 hra]# rm /mnt/config2/oradata/hra/control02.ctl
rm: remove regular file '/mnt/config2/oradata/hra/control02.ctl'? y
[root@node3 hra]# rm /mnt/config3/oradata/hra/control03.ctl
rm: remove regular file '/mnt/config3/oradata/hra/control03.ctl'? y

SQL> startup;
ORACLE instance started.
Total System Global Area 1002127360 bytes
Fixed Size                  2165888 bytes
Variable Size             750781312 bytes
Database Buffers          243269632 bytes
Redo Buffers                5910528 bytes
ORA-00205: error in identifying control file, check alert log for more info
Scenario 7: Recreate Dropped Table by Exporting It from Clone of Backup

In this scenario, a table is dropped and must be imported back from an existing full online backup. To restore only that table, first create a clone from the backup by using SnapManager. Then export the table from the clone database and manually import it back into the target database.

Using the GUI

To restore the table by using the GUI, complete the following steps:

1. Right-click Backup and select Clone.
2. Navigate through the rest of the wizard. Click Finish.
3. When the clone is complete, manually export the table from the clone:
   
   ```
   [oracle@tardb_host1][exp1][~]$ exp userid=user/password tables=sales file=sales12.dmp
   ```

4. When the export is complete, manually import the table into the target database:
   
   ```
   [oracle@tardb_host1][tardb1][~]$ imp userid=user/password tables=sales file=sales12.dmp
   ```

Using the CLI

To restore the table by using the CLI, complete the following steps:

1. Create a clone from the backup of the target database:
   
   ```
   smo clone create -profile targetdb1_prof1 -backup-label full_bkup_sales_apr_12 -newsid exp1 -clonespec ./smo/sales_clonespec.xml -reserve no -label sales0608_exp1 -verbose
   ```

2. When the clone is complete, manually export the table from the clone:
   
   ```
   [oracle@tardb_host1][exp1][~]$ exp userid=user/password tables=sales file=sales12.dmp
   ```

3. When the export is complete, manually import the table into the target database:
   
   ```
   [oracle@tardb_host1][tardb1][~]$ imp userid=user/password tables=sales file=sales12.dmp
   ```

Scenario 8: Recreate Dropped Table from Clone of Backup Using Database Link

In this scenario, a table is dropped and must be recreated from an existing full online backup. To recreate just that table, first create a clone from the backup by using SnapManager. Then manually create a database link from the target database to the clone and recreate the table in the target database by using the link.

Using the GUI
To restore the table by using the GUI, complete the following steps:

1. Right-click Backup and select Clone.
2. Navigate through the rest of the wizard. Click Finish.
3. When the clone is complete, manually add an entry for the clone database (for example, apr12cln) in the tnsnames.ora file.
4. Create a database link in the target database to the clone database:

   ```sql
   SQL> create public database link apr12_clone
   connect to sales identified by salespw
   using apr12cln
   ```

5. Recreate the dropped table in the target database by selecting it from the table in the clone database using the database link:

   ```sql
   SQL> create table europe_sales as
   2   select * from europe_sales@apr12_clone;
   ```

Using the CLI

To restore the table by using the CLI, complete the following steps:

1. Create a clone from the backup of the target database:

   ```bash
   smo clone create -profile targetdb1_prof1 -backup-label full_bkup_sales_apr_12-newsid expl
   -clonespec ./smo/sales_clonespec.xml -reserve no -label sales_expl -verbose
   ```

2. When the clone creation is complete, manually add an entry for the clone database (for example, apr12cln) in the tnsnames.ora file.
3. Create a database link in the target database to the clone database:

   ```sql
   SQL> create public database link apr12_clone
   Connect to sales identified by salespw
   using apr12cln
   ```

4. Recreate the dropped table in the target database by selecting it from the table in the clone database using the database link:

   ```sql
   SQL> create table europe_sales as
   2   select * from europe_sales@apr12_clone;
   ```

5 Conclusion

SnapManager 3.4 for Oracle offers a rich feature set that enables IT organizations to take advantage of fast, space-efficient, disk-based backups; rapid, granular restore and recovery; and quick, space-efficient cloning. The recommendations and examples in this report help users obtain maximum value from SMO deployments on NetApp storage. For more information about any of the solutions or products covered in this report, go to the NetApp Support site.

Appendixes

Appendix A: Sample Database Volume Layouts

<table>
<thead>
<tr>
<th>File Types</th>
<th>Volume Names</th>
<th>Dedicated</th>
<th>Automatic Snapshot Copies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle binaries</td>
<td>orabin_&lt;hostname&gt;</td>
<td>Yes</td>
<td>On</td>
</tr>
<tr>
<td>File Types</td>
<td>Volume Names</td>
<td>Dedicated</td>
<td>Automatic Snapshot Copies</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------</td>
<td>-----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Data files</td>
<td>oradata_&lt;sid&gt;</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Temporary data files</td>
<td>Oratemp_&lt;sid&gt;</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Control files</td>
<td>oracntrl01_&lt;sid&gt; (Multiplexed)</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Redo logs</td>
<td>oralog01_&lt;sid&gt; (Multiplexed)</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Archive logs</td>
<td>Oraarch_&lt;sid&gt;</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>RAC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Types</td>
<td>Volume Names</td>
<td>Dedicated</td>
<td>Automatic Snapshot Copies</td>
</tr>
<tr>
<td>Oracle binaries</td>
<td>orabin_&lt;hostname&gt;</td>
<td>Yes</td>
<td>On</td>
</tr>
<tr>
<td>Data files</td>
<td>oradata_&lt;dbname&gt;</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Temporary data files</td>
<td>oratemp_&lt;dbname&gt;</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Control files</td>
<td>oracntrl01_&lt;dbname&gt; (Multiplexed)</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Redo logs</td>
<td>oralog01_&lt;dbname&gt; (Multiplexed)</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Archive logs</td>
<td>oraarch_&lt;dbname&gt;</td>
<td>Yes</td>
<td>Off</td>
</tr>
<tr>
<td>Cluster files</td>
<td>oracrs_&lt;clusternname&gt;</td>
<td>Yes</td>
<td>On</td>
</tr>
<tr>
<td>ASM Single Instance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Types</td>
<td>Volume Names</td>
<td>LUNs</td>
<td>Dedicated</td>
</tr>
<tr>
<td>Oracle binaries</td>
<td>orabin_&lt;hostname&gt;</td>
<td>orabin_&lt;hostname&gt;.lun</td>
<td>Yes</td>
</tr>
<tr>
<td>Data files</td>
<td>oradata_&lt;sid&gt;</td>
<td>oradata_&lt;sid&gt;.lun</td>
<td>Yes</td>
</tr>
<tr>
<td>Temporary data files</td>
<td>oratemp_&lt;sid&gt;</td>
<td>oratemp_&lt;sid&gt;.lun</td>
<td>Yes</td>
</tr>
<tr>
<td>Control files</td>
<td>oracntrl01_&lt;sid&gt; (Multiplexed)</td>
<td>oracntrl01_&lt;sid&gt;.lun (Multiplexed)</td>
<td>Yes</td>
</tr>
<tr>
<td>Redo logs</td>
<td>oralog01_&lt;sid&gt; (Multiplexed)</td>
<td>oralog01_&lt;sid&gt;.lun (Multiplexed)</td>
<td>Yes</td>
</tr>
<tr>
<td>Archive logs</td>
<td>oraarch_&lt;sid&gt;</td>
<td>oraarch_&lt;sid&gt;.lun</td>
<td>Yes</td>
</tr>
<tr>
<td>ASM RAC</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Perform Block-Level Restore Using RMAN

This appendix is an overview of the tasks involved in backing up a database using SnapManager for Oracle (SMO) and performing a block-level recovery of that database using Oracle Recovery Manager (RMAN).

This process provides an overview of how to back up a database and perform block-level recovery of that database using RMAN:

1. Perform a backup (this example uses a full offline backup) of the database by using SMO.
2. Verify that the backup is cataloged with RMAN.
3. Review the backup to determine whether any blocks were corrupted.
4. Mount the backup by using SnapManager to make it accessible to RMAN.
5. Use RMAN to perform the block-level restore.
6. Verify that the corrupted blocks were repaired.

To back up a database and perform a block-level recovery of that database by using RMAN, complete the following detailed steps:

1. Perform a full offline backup by using SnapManager:

   smo backup create -profile <profile_name> -data -retain -hourly -offline -force -verbose

   Where:
   Profile_name is the name of the profile with which backup is associated
   Example:
   smo backup create -profile HRA -data -retain -hourly -offline -force -verbose

   Output:
   [ INFO] SMO-07109: Cataloguing all files in backup set with RMAN, TAG=SMO_D_C_20120522_1337665850563, RMAN=rman@db2/catalog.
   [ INFO] ORACLE-20000: Changing state for database instance hra from MOUNTED to OPEN.
   [ INFO] ORACLE-20032: Opening database hra with READ WRITE option.
   [ INFO] SMO-13048: Backup Create Operation Status: SUCCESS
   [ INFO] SMO-13049: Elapsed Time: 0:03:12.770
   Operation Id [8ac847c8377316f001377316f70d0001] succeeded.
2. Verify that the backup is cataloged with RMAN. At the RMAN prompt from the database host, enter this command:

```
RMAN> list datafilecopy tag <tagname>;
Example:
RMAN> list datafilecopy tag SMO_D_C_20120522_1337665850563;
```

<table>
<thead>
<tr>
<th>Key</th>
<th>File S Completion Time</th>
<th>Ckp SCN</th>
<th>Ckp Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>751</td>
<td>1</td>
<td>A 22-MAY-12</td>
<td>1883562</td>
</tr>
<tr>
<td></td>
<td>Name: /opt/NetApp/imo/mnt/-mnt-nfs1-20120522112023977_0/oradata/hra/system01.dbf</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tag: SMO_D_C_20120522_1337665850563</td>
<td></td>
<td></td>
</tr>
<tr>
<td>747</td>
<td>2</td>
<td>A 22-MAY-12</td>
<td>1883562</td>
</tr>
<tr>
<td></td>
<td>Name: /opt/NetApp/imo/mnt/-mnt-nfs1-20120522112023977_0/oradata/hra/sysaux01.dbf</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tag: SMO_D_C_20120522_1337665850563</td>
<td></td>
<td></td>
</tr>
<tr>
<td>746</td>
<td>3</td>
<td>A 22-MAY-12</td>
<td>1883562</td>
</tr>
<tr>
<td></td>
<td>Name: /opt/NetApp/imo/mnt/-mnt-nfs1-20120522112023977_0/oradata/hra/undotbs01.dbf</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tag: SMO_D_C_20120522_1337665850563</td>
<td></td>
<td></td>
</tr>
<tr>
<td>748</td>
<td>4</td>
<td>A 22-MAY-12</td>
<td>1883562</td>
</tr>
<tr>
<td></td>
<td>Name: /opt/NetApp/imo/mnt/-mnt-nfs1-20120522112023977_0/oradata/hra/users01.dbf</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tag: SMO_D_C_20120522_1337665850563</td>
<td></td>
<td></td>
</tr>
<tr>
<td>749</td>
<td>5</td>
<td>A 22-MAY-12</td>
<td>1883562</td>
</tr>
<tr>
<td></td>
<td>Name: /opt/NetApp/imo/mnt/-mnt-nfs1-20120522112023977_0/oradata/hra/example01.dbf</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tag: SMO_D_C_20120522_1337665850563</td>
<td></td>
<td></td>
</tr>
<tr>
<td>750</td>
<td>6</td>
<td>A 22-MAY-12</td>
<td>1883562</td>
</tr>
<tr>
<td></td>
<td>Name: /opt/NetApp/imo/mnt/-mnt-nfs1-20120522112023977_0/oradata/hra/test01.dbf</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tag: SMO_D_C_20120522_1337665850563</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Assuming that the data file `users01.dbf` is corrupted, run `dbverify`:

```
dbverify file=filename.dbf
Example:
    dbverify file= /mnt/nfs1/oradata/hra/users01.dbf
```

Output:
```
DBVERIFY - Verification starting : FILE = /mnt/nfs1/oradata/hra/users01.dbf
Page 163 is marked corrupt
Corrupt block relative dba: 0x010000a3 (file 4, block 163)
Bad header found during dbv:
Data in bad block:
  type: 109 format: one rdba: 0x20746920
  last change scn: 0x7075.72726f63 seq: 0x74 flg: 0x0a
  spare1: 0x66 spare2: 0x65 spare3: 0x0
  consistency value in tail: 0x00000001
  check value in block header: 0xa6a3
  block checksum disabled
```

Page 164 is marked corrupt
```
Corrupt block relative dba: 0x010000a4 (file 4, block 164)
Bad header found during dbv:
Data in bad block:
  type: 109 format: 1 rdba: 0x20746920
  last change scn: 0x7075.72726f63 seq: 0x74 flg: 0x0a
  spare1: 0x66 spare2: 0x65 spare3: 0x0
  consistency value in tail: 0x00000001
  check value in block header: 0xa6a4
  block checksum disabled
DBVERIFY - Verification complete
```
Total Pages Encrypted : 0
Highest block SCN : 909663 (0.909663)

Note: Two pages are marked as corrupt.

4. Mount the backup by using SMO to make it accessible to RMAN:

```plaintext
smo backup mount -profile <profile_name> -label <backup_label_name> -verbose
Example:
smo backup mount -profile HRA -label D_C_20120522112023982 -label D_C_20120522112023982 -label D_C_20120522112023982 -label D_C_20120522112023982
Output:
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config3-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config3-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config1-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config1-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config2-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config2-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-nfs1-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-nfs1-20120522112023982
[ INFO] SD-00026: Finished connecting filesystem(s) [/mnt/config3, /mnt/config1, /mnt/config2, /mnt/nfs1] from snapshot smo_hra_rman_hra_d_c_1_8ac847c8377316f0013773167f70d0001_0.
[ INFO] SD-00026: Finished connecting filesystem(s) [/mnt/config3, /mnt/config1, /mnt/config2, /mnt/nfs1] from snapshot smo_hra_rman_hra_d_c_1_8ac847c8377316f0013773167f70d0001_0.
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config3-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config3-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config1-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config1-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config2-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config2-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-nfs1-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-nfs1-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config3-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config3-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config1-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config1-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-config2-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-config2-20120522112023982
[ INFO] SD-00016: Discovering storage resources for /opt/NetApp smo/mnt/mnt-nfs1-20120522112023982
[ INFO] SD-00017: Finished storage discovery for /opt/NetApp smo/mnt/mnt-nfs1-20120522112023982
[ INFO] SD-00026: Finished connecting filesystem(s) [/mnt/config3, /mnt/config1, /mnt/config2, /mnt/nfs1] from snapshot smo_hra_rman_hra_d_c_1_8ac847c8377316f0013773167f70d0001_0.
[ INFO] SD-00026: Finished connecting filesystem(s) [/mnt/config3, /mnt/config1, /mnt/config2, /mnt/nfs1] from snapshot smo_hra_rman_hra_d_c_1_8ac847c8377316f0013773167f70d0001_0.
[ INFO] SMO-13048: Backup Mount Operation Status: SUCCESS
Output:
[ INFO] SMO-13049: Elapsed Time: 0:00:34.441
Operation Id [8ac847c83773471b01377347234a0001] succeeded.
```

5. Use RMAN to perform a block-level restore:

```plaintext
RMAN> blockrecover datafile '</mnt/path/file.dbf>' block <block_id> from tag <backup_rman_tag>
Example:
RMAN> blockrecover datafile '/mnt/nfs1/oradata/hra/users01.dbf' block 163,164 from tag SMO_D_C_20120522112023982
Starting recover at 22-MAY-12
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=134 device type=DISK
channel ORA_DISK_1: restoring block(s) from datafile copy /opt/NetApp smo/mnt/mnt-nfs1-20120522112023982/oradata/hra/users01.dbf
starting media recovery
media recovery complete, elapsed time: 00:00:01
Finished recover at 22-MAY-12
```

6. Verify that the corrupted blocks have been repaired by using dbverify again:

```plaintext
dbv file=filename.dbf
Example:
dbv file= /mnt/nfs1/oradata/hra/users01.dbf
Output:
[oracle@node3 ~]$ dbv file=/mnt/nfs1/oradata/hra/users01.dbf
DBVERIFY: Release 11.1.0.7.0 - Production on Tue May 22 12:18:27 2012
Copyright (c) 1982, 2007, Oracle. All rights reserved.
DBVERIFY - Verification starting : FILE = /mnt/nfs1/oradata/hra/users01.dbf
DBVERIFY - Verification complete
Total Pages Examined : 640
Total Pages Processed (Data) : 91
Total Pages Failing (Data) : 0
Total Pages Processed (Index) : 33
Total Pages Failing (Index) : 0
Total Pages Processed (Other) : 496
Total Pages Processed (Seg) : 0
Total Pages Failing (Seg) : 0
```

Appendix C: Tablespace Point-in-Time Recovery Using RMAN

This section is an overview of the tasks involved in backing up a database using SnapManager for Oracle (SMO) and performing a tablescape point-in-time recovery of that database using Oracle Recovery Manager (RMAN).

This process provides an overview of how to back up a database and perform a tablescape point-in-time recovery of that database:

1. Perform a backup (this example uses a full online backup) of the database by using SMO.
2. Find the SCN and time stamp until the point of recovery to be performed and bring the tablescape offline. Verify that the backup is cataloged with RMAN and mount the backup by using SnapManager to make it accessible to RMAN.
3. Perform the tablescape point-in-time recovery by using RMAN.
4. Bring the tablescape online and verify the data.

To back up a database and perform a tablescape point-in-time recovery of that database, complete the following detailed steps:

1. Perform a backup (this example uses a full online backup) of the database by using SMO:

   ```sql
   SQL> select count(*) from i2et1;
   COUNT(*)  
   --------
   7
   ```
2. Find the SCN and time stamp until the point of recovery to be performed (SCN=2928299 and TIMESTAMP=07-JUN-12 12.03.00PM, in the following example) and bring the tablespace offline:

```sql
SQL> insert into i2et1 select * from i2et1;
  7 rows created.
SQL> /
 14 rows created.
SQL> /
28 rows created.
SQL> /
56 rows created.
SQL> select count(*) from i2et1;
COUNT(*) -------
112
SQL> select current_scn from v$database;
CURRENT_SCN -------
2928299
SQL> commit;
Commit complete.
SQL> insert into i2et1 select * from i2et1;
112 rows created.
SQL> select count(*) from i2et1;
COUNT(*) -------
224
SQL> select current_scn from v$database;
CURRENT_SCN -------
2928395
SQL> commit;
Commit complete.
SQL> insert into i2et1 select * from i2et1;
112 rows created.
SQL> select count(*) from i2et1;
COUNT(*) -------
224
SQL> select current_scn from v$database;
CURRENT_SCN -------
2928395
SQL> commit;
Commit complete.
```

3. Verify that the backup is cataloged with RMAN:

```sql
RMAN> list datafilecopy tag "SMO_D_A_20120607_1339050439386";
starting full resync of recovery catalog
full resync complete
List of Datafile Copies
-------------------------------
Key File S Completion Time Ckp SCN Ckp Time
----------------- ----------------- ----------------- -----------------
5177 1 A 07-JUN-12 2927089 07-JUN-12
      Name: /opt/NetApp/sm0/mnt/-mnt-nfst/20120607115650287_0/oradata/hra/system01.dbf
      Tag: SMO_D_A_20120607_1339050439386
5173 2 A 07-JUN-12 2927089 07-JUN-12
      Name: /opt/NetApp/sm0/mnt/-mnt-nfst/20120607115650287_0/oradata/hra/sysaux01.dbf
      Tag: SMO_D_A_20120607_1339050439386
5175 3 A 07-JUN-12 2927089 07-JUN-12
      Name: /opt/NetApp/sm0/mnt/-mnt-nfst/20120607115650287_0/oradata/hra/undotbs01.dbf
      Tag: SMO_D_A_20120607_1339050439386
5176 4 A 07-JUN-12 2927089 07-JUN-12
      Name: /opt/NetApp/sm0/mnt/-mnt-nfst/20120607115650287_0/oradata/hra/users01.dbf
      Tag: SMO_D_A_20120607_1339050439386
5174 5 A 07-JUN-12 2927089 07-JUN-12
      Name: /opt/NetApp/sm0/mnt/-mnt-nfst/20120607115650287_0/oradata/hra/example01.dbf
      Tag: SMO_D_A_20120607_1339050439386
5178 6 A 07-JUN-12 2927089 07-JUN-12
```
4. Mount the backup by using SnapManager to make it accessible to RMAN. Make sure that all the required archive logs are available at the archive log destination.
   - If the archive logs were pruned during the previous backup, mount the archive log backup and copy the archive logs manually to the archive log destination.

5. Use RMAN to perform the tablespace point-in-time recovery.

   ```sql
   RMAN> recover tablespace i2e until time "to_date('2012-06-07 12.03.00', 'YYYY-MM-DD HH24:MI:SS')"
   auxiliary destination '/tmp'.
   . . importing SYS's objects into SYS
   . . importing table "I2ET1"
   Import terminated successfully without warnings.
   host command complete
   sql statement: alter tablespace I2E online
   starting full resync of recovery catalog
   full resync complete
   sql statement: alter tablespace I2E offline
   starting full resync of recovery catalog
   full resync complete
   sql statement: begin dbms_backup_restore.AutoBackupFlag(TRUE); end;
   starting full resync of recovery catalog
   full resync complete
   Removing automatic instance
   Automatic instance removed
   auxiliary instance file /tmp/TSPITR_HRA_SFFT/onlinelog/ol_mf_3_7x0wvc66_.log deleted
   auxiliary instance file /tmp/TSPITR_HRA_SFFT/onlinelog/ol_mf_2_7x0wvbjq_.log deleted
   auxiliary instance file /tmp/TSPITR_HRA_SFFT/onlinelog/ol_mf_1_7x0wv93y_.log deleted
   auxiliary instance file /tmp/TSPITR_HRA_SFFT/datafile/ol_mf_temp_7x0wvfr9n_.tmp deleted
   auxiliary instance file /tmp/TSPITR_HRA_SFFT/datafile/ol_mf_sysaux_7x0wtmww_.dbf deleted
   auxiliary instance file /tmp/TSPITR_HRA_SFFT/datafile/ol_mf_undotbs1_7x0wtjw0_.dbf deleted
   ```
6. Bring the tablespace online and verify the data.

```
SQL> alter tablespace i2e online;
Tablespace altered.
SQL> select count(*) from i2et1;
  COUNT(*) --------
          112
```

Appendix D: Clone RAC Database to Non-RAC Database and Convert It to RAC Database

SnapManager for Oracle (SMO) clones an Oracle Real Application Clusters (Oracle RAC) database to a non-RAC database and sets the Oracle parameter `cluster.database` to `false`.

To create a clone of a RAC database, complete the following steps:

1. Create a clone from a backup by using the SnapManager CLI:

   ```
   smo clone create -backup-label backup_label -profile <profile_name> -newsid <new_SID> -clonespec <full_path_to_clonespec_file> -verbose
   ```

2. When the cloning operation is complete, rename the `initclone_SID.ora` file as `initclone_local_instance_SID.ora`, edit the file, and set `cluster.database` to `true`.

3. Register the cloned RAC database with `srvctl`.

4. The following example sets up a cloned database as a one-node RAC instance. Use an editor, such as `vi`, to change the `.ora` file.

   ```
   $ smo clone create -backup-label rac_full_backup -profile rac_profile -newsid CLONE1 -clonespec rac_nfs_clonespec.xml -verbose
   $ export ORACLE_SID= CLONE1
   $ sqlplus / as sysdba;
   Shutdown immediate;
   $ vi initCLONE11.ora
   *cluster_database = TRUE
   CLONE11.instance_number = 1
   CLONE11.thread=1
   CLONE11.undo_tablespace='UNDOTBS1';
   $ srvctl add database -d CLONE1 -o /u02/app/oracle/product/10.2.0/db -m rtp.company.com -r primary -y manual
   $ srvctl add instance -d CLONE1 -i CLONE11 -n anzio
   $ srvctl start instance -d CLONE1 -i CLONE11
   ```

   **Note:** All the steps performed previously to turn this clone into a RAC database must be undone before attempting to delete the clone.

References

This report referenced the following documents and resources:

- Data ONTAP System Administration Guide
  https://support.netapp.com /documentation/productsatoz/index.html
- SnapManager 3.4 for Oracle Installation and Administration Guide
  https://library.netapp.com/ecm/ecm_download_file/ECMP1354397
- SnapManager 3.4 for Oracle Release Notes
  https://library.netapp.com/ecm/ecm_download_file/ECMP1354398
- SnapDrive 5.3 for UNIX Installation and Administration Guide (if Oracle is on UNIX)  
  [https://library.netapp.com/ecm/ecm_download_file/ECMP1393581](https://library.netapp.com/ecm/ecm_download_file/ECMP1393581)
- SnapDrive 7.0.1 for Windows Installation Guide (if Oracle is on Windows)  
  [https://library.netapp.com/ecm/ecm_download_file/ECMP1201909](https://library.netapp.com/ecm/ecm_download_file/ECMP1201909)
- OnCommand Unified Manager 5.2 Core Package Installation and Setup Guide  
  [https://library.netapp.com/ecm/ecm_download_file/ECMP1222478](https://library.netapp.com/ecm/ecm_download_file/ECMP1222478)
- Best Practice for Oracle Databases on NetApp Storage  
- NetApp Interoperability Matrix  
- NetApp Mount Options KB Article 3010189  
  [https://kb.netapp.com/support/index?page=content&id=3010189](https://kb.netapp.com/support/index?page=content&id=3010189)

### Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>April 2009</td>
<td>Initial release. Authors: Anand Ranganathan and Antonio Jose Rodrigues</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>October 2012</td>
<td>Document updated with new features available in SnapManager 3.2 for Oracle. Authors: Anand Ranganathan, Antonio Jose Rodrigues, and Himanshu Prashar</td>
</tr>
<tr>
<td>Version 1.2</td>
<td>June 2014</td>
<td>Document updated with new features available in SnapManager 3.3.1 for Oracle. Author: Himanshu Prashar</td>
</tr>
<tr>
<td>Version 2</td>
<td>July 2015</td>
<td>Document updated with new features and use cases along with structural changes and contents for SnapManager 3.4 for Oracle. Authors: Ebin Kadavy, Jeffrey Steiner, Antonio Jose Rodrigues Neto, and Anand Ranganathan</td>
</tr>
</tbody>
</table>
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC. SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, WAFL and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the Web at http://www.netapp.com/us/legal/netapptmlist.aspx. TR-3761-0715