Technical Report

SnapCenter Plug-In for Oracle Database

Best Practices

Ebin Varghese Kadavy and SnapCenter Engineering, NetApp

February 2021 | TR-4700

Abstract

NetApp® SnapCenter® is a unified, scalable platform for Oracle-consistent data protection that automates complex operations with centralized control and oversight. This report explains the best practices for deploying Oracle databases with SnapCenter.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Introduction

In today's data-driven enterprise, business-critical applications must be operational around the clock to facilitate decision making, e-commerce, and many other business processes. Virtualization has improved significantly and in recent years has gradually become the platform of choice for tier 1 applications. Customers who use enterprise applications such as Oracle, Microsoft SQL Server, PostgreSQL, and MYSQL are starting to choose virtualization over physical deployments.

Oracle databases are among the most important applications in many environments. Relational databases are used for custom applications developed internally by a company, or as a database back end for commercial application deployments. In both scenarios, data registered in Oracle databases requires proper design to be readily available. Rapid growth in data volume and application demands makes it increasingly difficult to provide availability and protection for valuable data assets.

Administrators need tools that enable them to take frequent backups with minimal impact on operations, perform quick application recovery, and rapidly create copies for user testing and development regardless of physical, virtual, or hybrid cloud deployments. SnapCenter data protection software offers a high degree of availability for Oracle databases by leveraging its capabilities such as data loss avoidance, verified protection, and high-speed recovery.

Audience

This document is intended for use by customers who are using Oracle databases either in physical or virtualized environments or mix of both of them. It is a source of useful information about best practices on data protection for Oracle databases for storage administrators, database administrators, virtualization specialists, architects, and data protection administrators.

Purpose

This document describes the best practices for deploying and ensuring data availability of Oracle deployments on NetApp ONTAP® storage running in an on-premises, co-located data center or cloud and for leveraging SnapCenter Plug-In for Oracle. The recommendations in this report are generic; they are not specific to any configuration and, depending on your business needs, some suggestions might require changes. Each environment should be carefully evaluated against the NetApp Interoperability Matrix Tool (IMT), official documentation for SnapCenter, ONTAP storage, hypervisors, and Oracle Database.

SnapCenter and Plug-in for Oracle overview

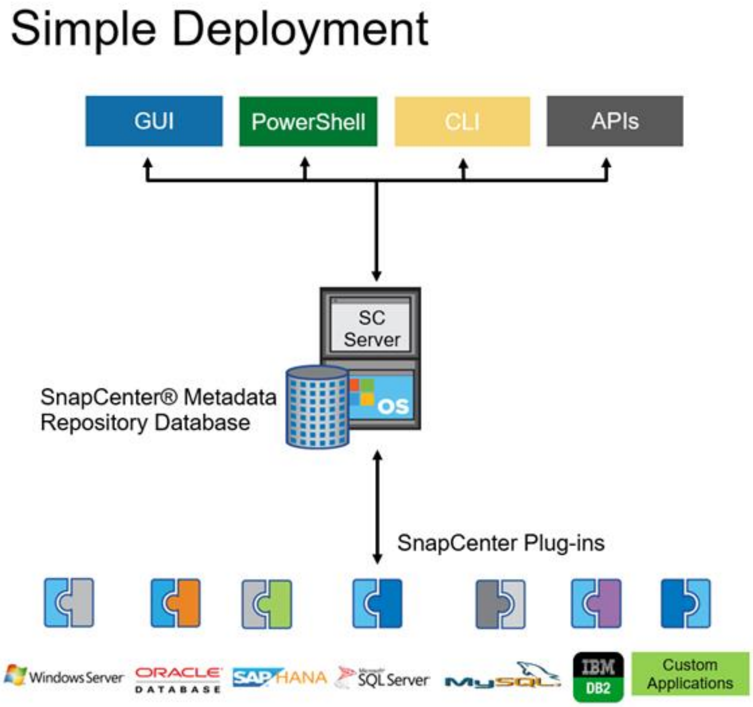
SnapCenter is NetApp's next-generation data protection software for enterprise applications. With its "single pane of glass" management interface, SnapCenter automates and simplifies the manual, complex, and time-consuming processes associated with the backup, recovery, and cloning of multiple databases and other application workloads.

SnapCenter leverages NetApp technologies, including Snapshot™ copies, SnapMirror® replication software, SnapRestore® data recovery software, and FlexClone® volumes, which allow it to integrate seamlessly with databases and hypervisors across FC, FCoE, iSCSI, and NAS protocols. This integration allows IT organizations to scale their storage infrastructure, meet increasingly stringent SLA commitments, and improve the productivity of administrators across the enterprise.

Architecture and concepts

Figure 1 shows the SnapCenter architecture.

Figure 1) SnapCenter architecture.



SnapCenter Plug-in for Oracle comes with three user interfaces: CLI, GUI, and PowerShell.

The SnapCenter metadata repository database (MySQL open source) is an integral part of SnapCenter that gets deployed and configured as part of the SnapCenter installation. It holds the host and file systems details, backup, restore, and clone metadata of each resource that is being protected.

SnapCenter Server can be scaled to support high availability and load balancing with the help of external Load Balancer (F5 was qualified officially as of 4.3.2). Few customers have deployed SnapCenter high availability in a VMware HA+FT deployment.

SnapCenter Plug-In for Oracle has two major components:

- **SMCore** is a core component of SnapCenter that runs co-located within the SnapCenter Server host, unlike other plug-ins. This component plays a significant role in invoking and handling all the major workflows, starting with discovering the storage devices, hosting the file system, secondary replication of backups, and retention management. SMCore coordinates with the Linux Plug-In (managed by the SnapCenter Plug-in loader [SPL]) to perform Oracle Database workflows.
- **SPL** is a component that runs on the Oracle Database host that loads and runs the Oracle plug-in. SMCore coordinates with SPL to perform Oracle data protection workflows such as quiesce/unquiesce, backup, RMAN catalog, mount, restore, and clone.

Supported and unsupported features

SnapCenter Plug-in for Oracle supports or compliments the following ONTAP key functionalities (as of 4.4 release):

- AutoSupport
- NFS, iSCSI, FC, and FCoE protocols
- FabricPool
- NetApp Flash Cache

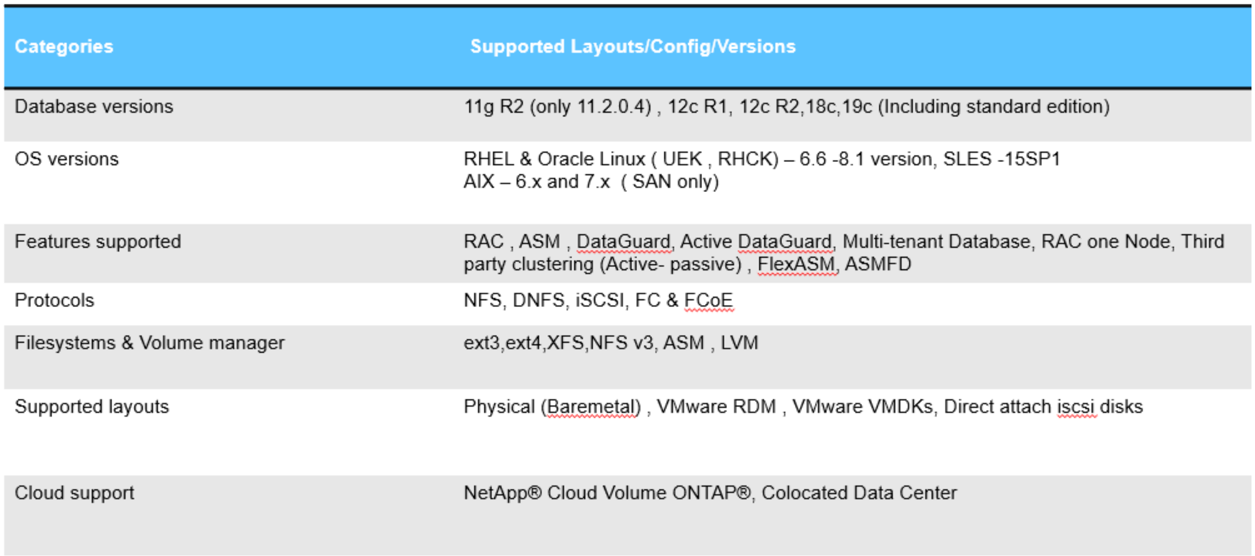
- NetApp Flash Pool aggregates
- NetApp MetroCluster (fabric and IP)
- SnapMirror/SnapVault® technology
- NetApp SnapRestore software
- Snapshot copies
- Storage efficiency using deduplication, compression, and compaction
- NetApp Volume Encryption (NVE)
- Volume move /LUN move (older backups will not work in a LUN move, even for volume rename)

SnapCenter Plug-in for Oracle does not support the following functionalities:

- Auto-balance aggregate
- NetApp ONTAP FlexGroup volumes
- Infinite volumes
- Volume renaming (supported for new backups)
- LUN renaming
- NetApp antivirus (Vscan)
- NetApp SnapLock®
- SNMP
- Storage virtual machine (SVM); disaster recovery
- Volume rehost
- Multifactor authentication
- SnapMirror Synchronous
- SMBC
- NetApp FlexCache technology
- NDMP
- LUN move (previously described)
- Multiple SAN initiator groups (igroups) for a single LUN

Figure 2 lists the supported Oracle features:

Figure 2) Supported Layouts, Configurations, versions, and features.



Categories	Supported Layouts/Config/Versions
Database versions	11g R2 (only 11.2.0.4) , 12c R1, 12c R2,18c,19c (Including standard edition)
OS versions	RHEL & Oracle Linux (UEK , RHCK) – 6.6 -8.1 version, SLES -15SP1 AIX – 6.x and 7.x (SAN only)
Features supported	RAC , ASM , DataGuard, Active DataGuard, Multi-tenant Database, RAC one Node, Third party clustering (Active- passive) , FlexASM, ASMFD
Protocols	NFS, DNFS, iSCSI, FC & FCoE
Filesystems & Volume manager	ext3,ext4,XFS,NFS v3, ASM , LVM
Supported layouts	Physical (Baremetal) , VMware RDM , VMware VMDKs, Direct attach iscsi disks
Cloud support	NetApp® Cloud Volume ONTAP®, Colocated Data Center

Note: For updated qualifications, see the NetApp IMT.

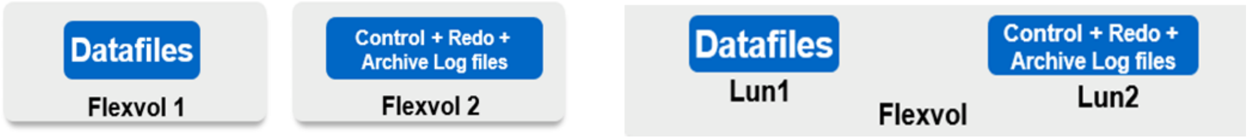
The unsupported Oracle features, file systems, and platforms include:

- Oracle Data Guard broker, Golden Gate
- RAC-to-RAC clone (only a RAC-to-nonRAC database clone is supported)
- Automatic Storage Management (ASM)-to-nonASM clone (cross file system clones are not supported)
- Cannot recognize Data Guard lifecycle such as switching standby to production or vice versa
- Disaster recovery automation and management of backups post failover or failback
- AIX NFS, Solaris, and Windows platforms
- Third-party volume managers (Veritas Volume Manager [VxVM])
- Oracle Automatic Storage Management Cluster (ACFS) file systems
- Encrypted file system, `autofs` (clone will not add an entry into `autofs` subsystem)
- Recovery of Data Guard and Active Data Guard
- Backup verification on remote host
- VMware vSphere Virtual Volumes (vVols)
- Virtual raw device mapping (RDM) is not a supported configuration; only physical RDM configuration is supported
- Oracle Transparent Data Encryption (TDE) deployments that are not auto-login mode
- Restore to alternate host
- Log backups of standby database (Data Guard/Active Data Guard)

Database storage best practices

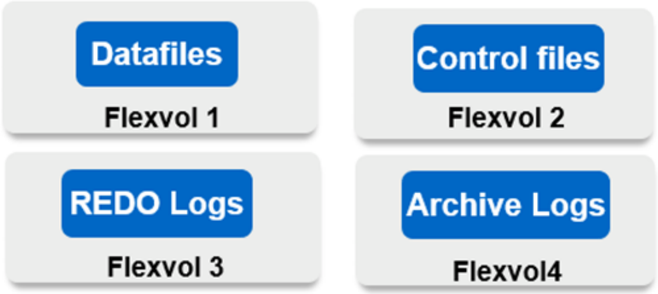
SnapCenter supports database environments backed by ONTAP storage that are mounted to the host as either physical or as virtual devices. You can host the entire database on a single or multiple storage devices based on the criticality of the environment. Typically customers would isolate the data files on a dedicated storage from all other files such as control files, and redo and archive log files. This helps administrators to quickly restore (ONTAP single-file SnapRestore) or clone a large critical database (petabyte scale) using Snapshot technology within few seconds to minutes.

Figure 3) Typical customer storage layout.


Datafiles
Flexvol 1
Control + Redo + Archive Log files
Flexvol 2
Datafiles
Lun1
Flexvol
Control + Redo + Archive Log files
Lun2

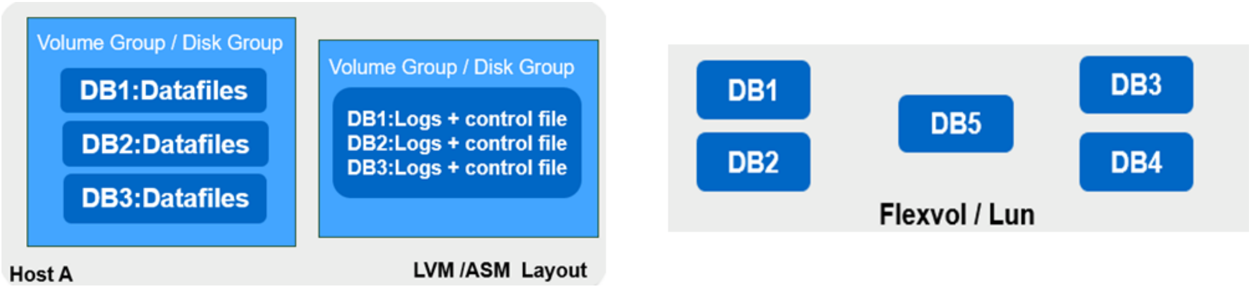
SnapCenter supports backup, restore and clone operations of large-scale databases (in petabytes) that are spawned across different aggregates and SVMs in the same or different clusters. Figure 4 is an example of a database environment that is hosted on dedicated storage volumes to benefit from latency limitations.

Figure 4)Dedicated storage layout.



SnapCenter also supports shared storage layouts in which you can host multiple databases or part of the databases on the same storage volume or LUN. A quick example of this layout would be that the data files of all the databases hosted on +DATA ASM disk group or volume group and the rest of the files (redo, archive log, and control files) on another dedicated disk group or volume group (LVM).

Figure 5) Shared storage layout.



It is important to note that the isolation discussed in the former scenario enables faster restore and recovery (using the ONTAP SnapRestore mechanism) unlike the shared storage layouts. When a database is shared on the same storage devices and when it is backed by a Snapshot, it is difficult to restore (using ONTAP SnapRestore) a specific database from the entire Snapshot copy. In this instance, SnapCenter leverages a FlexClone-based approach to perform connect and copy RMAN restore.

Best practices for shared and dedicated storage layouts

NetApp recommends the following best practices for shared and dedicated storage layouts:

- There is no challenge in restoring a database within an NFS storage environment (even though it is shared with other databases) because it can rapidly use ONTAP Single File SnapRestore to restore or revert the individual files instantly.
- In SAN, dedicated storage layout (mission-critical environment) is required for a quick restore. You must place Oracle data files in the dedicated volumes/LUNs with no other files such as physical copies of data files, backups, scripts, or plain text files, including other Oracle files.
- For SAN layouts, especially those running large databases with Oracle ASM, NetApp recommends keeping the disk group for the Oracle data files (DATA) in the separate volumes where LUNs or ASM disks are dedicated only for data files and not for any other files.
- One design consideration to reduce the storage footprint is to share the archive log destination for all the databases running in a host within the same volume/LUN as the Oracle flash recovery area (FRA) or non-FRA destination. When multiple databases of the same host are grouped in the same resource group for a backup, a single Snapshot copy is taken in the storage by consolidating the metadata for all the list of databases sharing the same storage.

Best practices for virtualized (NFS, VMFS, and RDM) environments

NetApp recommends the following best practices for virtualized environments:

- To execute a SnapCenter workflow such as backup, restore, and clone on a virtualized database environment (RDM/VMDK), you must first install and configure the SnapCenter Plug-in for VMware vSphere (SCV) OVA on a given vCenter and then register the Plug-in with SnapCenter Server.
- In general, there are numerous advantages of choosing NFS over VMware Virtual Machine File System (VMFS) datastore in terms of flexibility, cost, and data management. With SnapCenter, the restore of an entire database or pluggable databases (PDBs) backed by NFS datastore is extremely fast compared to a VMFS datastore. In an NFS scenario, the restore operation is performed at the ONTAP storage layer using Single File SnapRestore. In the case of VMFS, SnapCenter leverages VMware's storage vMotion to restore the files, hence it is slow for large databases.

  If databases reside on a VMDK, you must log into vCenter and navigate to VM Options > Advanced > Edit Configuration to set the value of `disk.enableUUID` to `true` for the VM. The VM must be rebooted after the change.
- SnapCenter doesn't allow you to back up the VMs and the Oracle application together. VMs must be backed up separately with different policies, using the SCV Plug-in. Oracle Database must be backed up from the SnapCenter GUI or CLI, or by using SnapCenter PowerShell cmdlets. There are few scenarios where a customer wants to back up both VM and Oracle Database together with application consistency. This backup can be done by including a simple pre- and post-script to quiesce and unquiesce Oracle Database while backing up spanned datastores.
- In RAC, there should be at least one dedicated VMware SCSI controller per VM to handle connect and copy restore.
- In the case of RAC environments, the restore of a virtualized database (VMDK/RDM) would be a connect and copy approach using ONTAP FlexClone files.

Additional resources

Oracle multitenancy is the future of Oracle databases. Starting from Oracle 12c, multitenancy came into limelight and eventually evolved in the later releases with lot of new features and offers a greater amount of consolidation thus helping in reducing the overall TCO. To learn more about the new best practices, see TR-4876: Oracle Multitenancy with ONTAP Solution and Deployment Best Practices.

Best practices for Oracle ASM configurations

NetApp recommends the following best practices for Oracle ASM configurations:

- For ASM layouts, make sure that the `ASM_DISKSTRING` value is set appropriately before handling any SnapCenter operations. If this value is not set correctly, then restore, clone, or mount operations fail:
  - If you are using the ASMLIB package for managing ASM devices, set the `ASM_DISKSTRING` value to `ORCL:*`.
  - For non ASMLIB scenarios such as `udev` rules, set the value to `/dev/< exact device location >`.
- SnapCenter doesn’t support ASM disks that have multiple partitions. It can only support disks with single or no partitions.
- User-defined multipath aliases along with a udev rule for ASM devices is not supported by SnapCenter. Either use multipath alias or use udev alias scheme for the devices.
- For ASMLIB or Oracle ASM Filter Driver (ASMFD), it is recommended not to use multipath aliases or udev aliases.
- 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’
ORACLEASM_USE_LOGICAL_BLOCK_SIZE=false
```

- If ASM without multipathing on Linux is used, make sure that `/etc/sysconfig/oracleasm` has the following variables set:

```
ORACLEASM_SCANORDER=’sd’
ORACLEASM_USE_LOGICAL_BLOCK_SIZE=false
```

- If you are using the following symlinks in udev rules for your ASM environment, run the following commands:

```
[root@asmrdmracn1 rules.d]# cat 99-oracle-asmdevices.rules
ENV{DM_NAME}=="3600a09803830454c695d4e724f483058",SYMLINK+="ASM_DISKS/gridmgmt",OWNER="grid",GROU
P="asmadmin",MODE="0660"
ENV{DM_NAME}=="3600a09803830454c695d4e724f473762",SYMLINK+="ASM_DISKS/oradata",OWNER="grid",GROUP
="asmadmin",MODE="0660"
ENV{DM_NAME}=="3600a09803830454c695d4e724f473763",SYMLINK+="ASM_DISKS/oralog",OWNER="grid",GROUP=
"asmadmin",MODE="0660"
```

  Then update the ASM_DISKSTRING as `/dev/ASM_DISKS/*`.

- The Oracle ASMFD is a kernel module that resides in the I/O path of the Oracle ASM disks. ASMFD is used to validate write I/O requests to Oracle ASM disks. Oracle ASMFD also simplifies the configuration and management of disk devices by eliminating the need to rebind disk devices used with Oracle ASM each time the system is restarted.
- ASMFD contains an incompatibility with many recent versions of Linux. Recent kernels enforce I/O size restrictions sent to multipath devices and ASMFD does not honor these restrictions. The result is that a database server configured with ASMFD will be unable to read drives.

  The solution is to manually specify the transfer length in the `multipath.conf` file for ONTAP LUNs:

```
devices {
            device {
                vendor "NETAPP"
                product "LUN.*"
                max_sectors_kb 4096
        }
    }
```

  Caution: Even if no problems currently exist, this parameter should be set to use ASMFD. Upgrades of Oracle, Linux, or ONTAP might result in the change to multipath devices that triggers the problem.

- If you are using the ASMFD for managing ASM devices, set the ASM_DISKSTRING value to AFD:*

- The restores can be slower in a flex ASM scenario when the cardinality is lower than the actual number of cluster nodes. To overcome this, ensure the ASM instance is running across all nodes by changing the cardinality value equal to the number of cluster nodes.
- SnapCenter cannot support protecting Oracle Database with ASM deployed over LVM .

SnapCenter Plug-in for Oracle preinstallation best practices

Preinstallation best practices cover requirements and prerequisites for both SnapCenter Server and the Oracle plug-in. Table 1 lists the minimum requirements and prerequisites to consider before installing a SnapCenter Server for managing Oracle environments.

Table 1) SnapCenter plug-in for Oracle scale requirements.

Item	Smaller environments	Larger environments	Very large environments
RAM (based on frequency of jobs on each host)	16G	32G	64G
CPU (>2.3 GHz)	4	8	8-12
Maximum number of backup jobs supported in parallel (backup concurrency)	20	40	80 (staggering of schedules can accommodate more database jobs)

Connection and port requirements

Table 2 lists the ports that must be enabled or freed from a firewall before installing SnapCenter Plug-in for Oracle software.

Table 2) Connection and port requirements.

Type of Port	Default port number and purpose
SnapCenter port (server)	8146 (HTTPS), bidirectional, customizable SnapCenter URL: https://<ip address or hostname>:8146 This port cannot be changed post-installation.
SnapCenter SMCore communication port (server)	8145 (HTTPS), bidirectional, customizable This port is used for communication between the SnapCenter Server and the hosts where the SnapCenter Plug-ins are installed.
Oracle plug-in	22 (SSH), not customizable This port is used by SnapCenter to copy plug-in package binaries to Linux plug-in hosts. They should be open or excluded from the firewall or iptables. Else perform manual installation of the plug-in on the Linux or AIX host and then later register the host with skip preinstall checks. 8145 port is used for communication between SMCore and hosts where the SnapCenter Plug-ins are installed. The communication path must be open between the SVM management LIF and SnapCenter Server.

SnapCenter expects its Linux host to be resolvable during the host registration process. If the Linux host or storage cannot be resolved to a fully qualified domain name (FQDN) for any reason (for example, the host coming from a different cloud, different domain, or private network), the workaround is to add an entry of the host or storage with a hostname (FQDN) in the `C:\Windows\System32\drivers\etc\hosts` file in Windows.

If you are adding a host running in any public cloud and you plan to manage databases (backup, restore, and clone) by using SnapCenter running in either a private data center or cloud, it is important to make sure that the firewall is open to listen to host IPs and ports 8145 and 8146 with inbound and outbound communication enabled. For example, if you want to clone an Oracle Database running on premises to Amazon Web Services (AWS) cloud, you must enable ports 8145 and 8146 bidirectionally, along with port 22 (SSH) to install the Linux plug-in on the Linux host running in the cloud. However, you can skip port 22 from the firewall list by manually copying and installing the plug-in directly to the Linux /AIX host. After manually installing the plug-in on the host, you must register the host with SnapCenter. While registering, select the Skip Prechecks option to register the Oracle host with SnapCenter.

To enable a port on the Linux host firewall settings such as RHEL 7.x,8.x use the following commands:

```
root> /sbin/iptables -A INPUT -p tcp -m tcp --dport 8145 -j ACCEPT
root> /sbin/iptables -A OUTPUT -p tcp -m tcp --dport 8145 -j ACCEPT
root> service iptables save
```

SnapCenter Plug-In for Oracle host requirements

Table 3) SnapCenter Plug-In for Oracle host requirements.

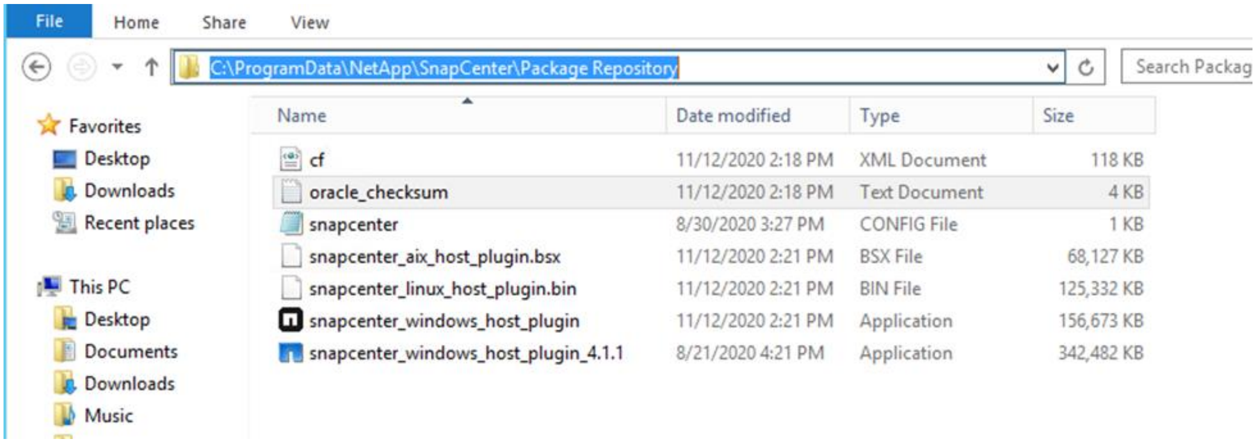
Item	Requirements
Operating systems	AIX, RHEL, Oracle Linux, SUSE For the latest information about supported versions, see the [NetApp Interoperability Matrix Tool (IMT)]().
Minimum memory for plug-in	Minimum 512MB Recommended 2–4GB (based on number of databases within the host)
Minimum installation and operational hard-drive space (for a minimum of three years)	Default installation location (binaries): `/opt/NetApp/SnapCenter` • Installation location can be customized (can also be on NetApp storage) • 3GB recommended Logs and config file location: `/var/opt/SnapCenter/` • Log location cannot be changed. • 20GB required (if logs are not pruned repeatedly and many databases being run within the same host)
Required software packages	• Java 1.8.x (64-bit) Oracle Java and OpenJDK If you are using multiple versions of Java for different applications, you must verify that the `JAVA_HOME` option is set to the correct Java path for SnapCenter; 32-bit java is not supported. • If LVM is used, then the LVM utils package must be installed. • For SAN environments, sg3_utils package is required.
Oracle plug-In installation user	Default Linux/AIX user is root

Item	Requirements
	Note: Nonroot accounts work, but sudo privileges are required for the nonroot account. Make sure that the sudo accounts have Oracle Database group privilege. NetApp recommends using a sudo package version 1.8.7 or later for checksums. SnapCenter has first-class integration with sudo only. However, if a user takes care of manually installing/upgrading the plug-in and ensures the services are always running as root user, it should work with pbrun framework as well. The plug-ins should work successfully.

In sudo user scenarios, add the following entries into `/etc/sudoers` file for your non-root user (scuser).

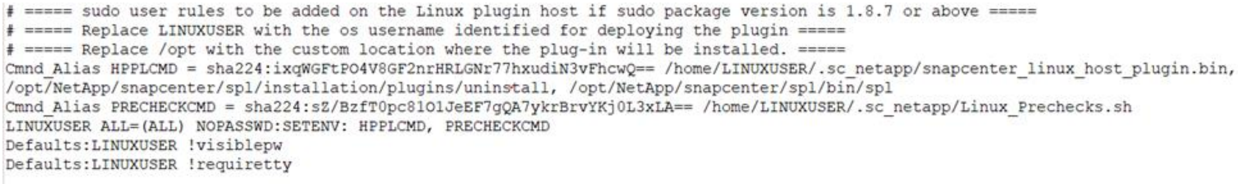
Navigate to the hidden directory and open the checksum file `oracle_checksum`.

```
C:\ProgramData\NetApp\SnapCenter\Package Repository
```

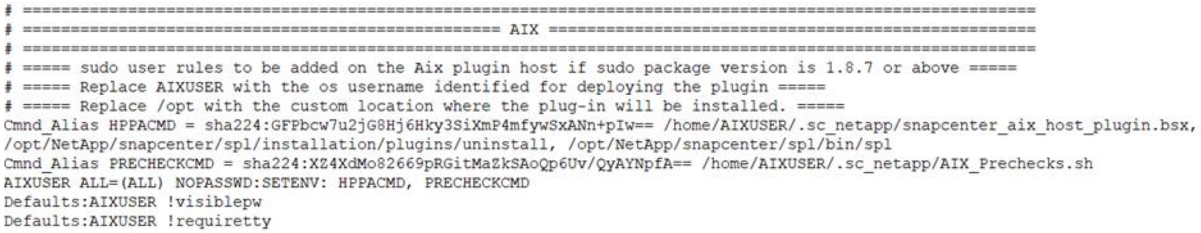


Name	Date modified	Type	Size
cf	11/12/2020 2:18 PM	XML Document	118 KB
oracle_checksum	11/12/2020 2:18 PM	Text Document	4 KB
snapcenter	8/30/2020 3:27 PM	CONFIG File	1 KB
snapcenter_aix_host_plugin.bsx	11/12/2020 2:21 PM	BSX File	68,127 KB
snapcenter_linux_host_plugin.bin	11/12/2020 2:21 PM	BIN File	125,332 KB
snapcenter_windows_host_plugin	11/12/2020 2:21 PM	Application	156,673 KB
snapcenter_windows_host_plugin_4.1.1	8/21/2020 4:21 PM	Application	342,482 KB

The checksum file can be edited to include the appropriate Linux or AIX user.



```
# ===== sudo user rules to be added on the Linux plugin host if sudo package version is 1.8.7 or above =====
# ===== Replace LINUXUSER with the os username identified for deploying the plugin =====
# ===== Replace /opt with the custom location where the plug-in will be installed. =====
Cmnd_Alias HPPLCMD = sha224:ixqWGFtPO4V8GF2nrHRLGNr77hxudiN3vFhcwQ== /home/LINUXUSER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall, /opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:sZ/BzfT0pc81O1JeEF7gQA7ykrBrvYKj0L3xLA== /home/LINUXUSER/.sc_netapp/Linux_Prechecks.sh
LINUXUSER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD
Defaults:LINUXUSER !visiblepw
Defaults:LINUXUSER !requiretty
```



```
# ==========================================================================================================
# ================================================== AIX ===================================================
# ==========================================================================================================
# ===== sudo user rules to be added on the Aix plugin host if sudo package version is 1.8.7 or above =====
# ===== Replace AIXUSER with the os username identified for deploying the plugin =====
# ===== Replace /opt with the custom location where the plug-in will be installed. =====
Cmnd_Alias HPPACMD = sha224:GFPbcw7u2jG8Hj6Hky3SiXmP4mfywSxANn+pIw== /home/AIXUSER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall, /opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:XZ4XdMo82669pRGitMaZkSAoQp6Uv/QyAYNpfA== /home/AIXUSER/.sc_netapp/AIX_Prechecks.sh
AIXUSER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD
Defaults:AIXUSER !visiblepw
Defaults:AIXUSER !requiretty
```

After the Oracle plug-in is running in the Oracle host, the rest of the communication from server to host or vice versa is only through REST API calls and not through the OS account.

Ensure that the `/etc/oratab` file has the correct Oracle home entries for each standalone database. SnapCenter discovers the details of the database only from this location. However, this setting is not required for RAC databases because of auto discovery enhancement that has been incorporated with the recent releases. Also, Ensure the Oracle Server Control (SRVCTL) utility is configured rightly for all RAC and ASM environments.

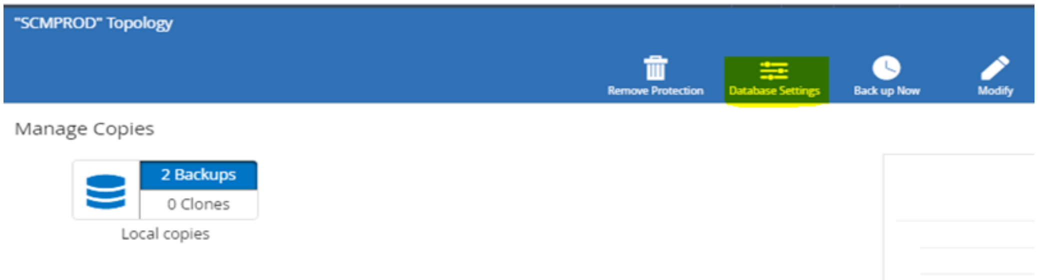
Note: If you are hosting an Oracle Database on a third-party host clustering solution which are not active-active such as Red Hat clustering or SIOS cluster then you need to register Oracle Database host through virtual IP (VIP) instead of a public IP or host name. For more information, see Appendix B: RAC one node and other third-party cluster solutions (active-passive).

SnapCenter backup policies and resource group best practices

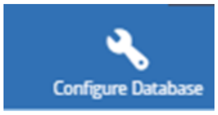
In SnapCenter terms, RPO can be identified as the backup frequency; that is, how frequently you schedule the backup to reduce data loss. The best practice is to schedule archive log backups more frequently than data backups or full backups. The minimum interval can be as short as 15 minutes for log backup. It is essential to note that frequent intervals of backup might also put you at the risk of hitting the limit of 1,024 Snapshot copies per volume. Effective retention strategy plays an important role in the backup policy and resource group design. One good example is to have multiple policies with different SLOs and retention limit and assign to the resource group.

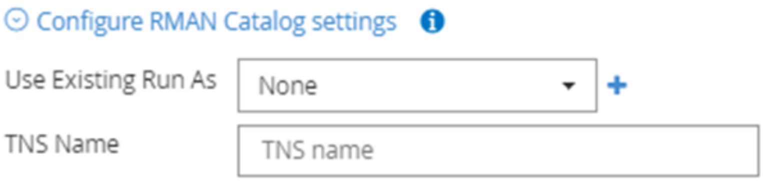
SnapCenter supports both online and offline backups. The full backup captures data files, archive logs, and control files with exception to data guard environments. To back up a Data Guard database (RAC or non-RAC), the policy should have the backup type set to Offline Mount Backup. For an Active Data Guard database, the backup type should be Online.

- **SnapMirror replication.** Protecting the Snapshot copies to a secondary storage is essential, therefore you must replicate your backups to a SnapMirror destination. SnapCenter doesn’t create a SnapMirror replication relationship, hence it must be done outside of SnapCenter. After the relationship is created, select the option for SnapMirror to replicate the backups. Retention for backups replicated in secondary storage must be handled directly from ONTAP. If you have enabled unified replication — that is, both mirror and vault replication — then backups are shown in both the mirror and vault destinations in the topology view.
- **Backup verification.** An optional feature that can be used to validate the files that are part of the backup. Verification can be enabled in the backup policy and activated during the protection workflow. You can verify the backups from both primary and secondary SnapMirror storage. You can also defer the verification by scheduling it for a later time from either the GUI or the CLI. During verification, a FlexClone volume is created from the backup and mounted to the host, and the Oracle `dbv` utility is run across all the data files present in the newly mounted FlexClone volume.
- **RMAN catalog of NetApp Snapshot copies.** SnapCenter provides an additional option to catalog and uncatalog the NetApp Snapshot copies with Oracle RMAN. This optional feature provides many great benefits to database administrators (DBAs), particularly in granular restores and recoveries such as block-level recovery, table recovery, individual data file recovery, and so on. The process involves creating and mounting the FlexClone of the data and log files volumes and later executing RMAN catalog command against the mounted FlexClone volume to capture the metadata. SnapCenter backup can be cataloged either on the target control file or the catalog database. If you leave catalog settings unconfigured, then SnapCenter, by default, catalogs the backups only with the target control file. Follow these steps to configure the catalog database connectivity.
    a. Go to Topology view of a database > Database Settings > Configure Database.
    b. Click Database Settings.



c. Click Configure Database to update the settings.





Use Existing Run As: None

TNS Name: TNS name

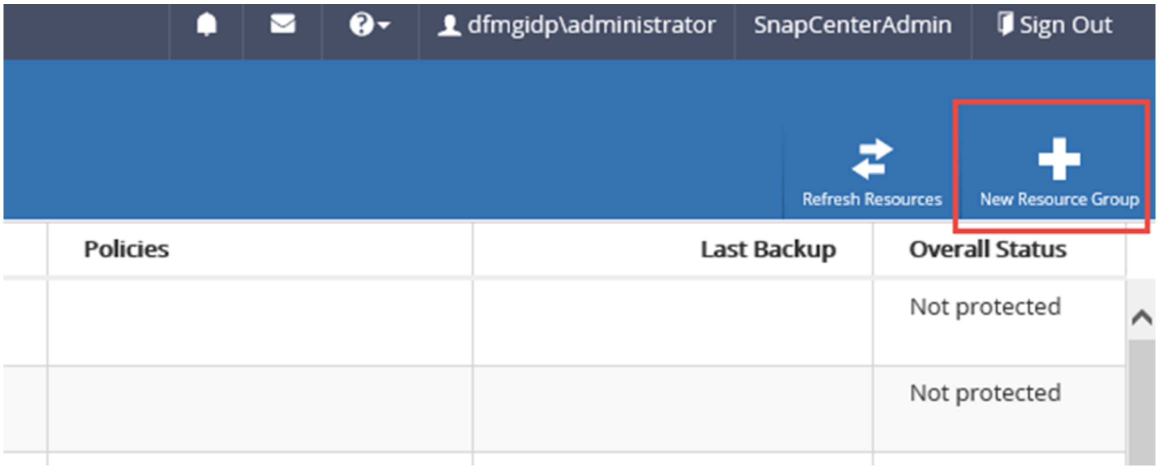
If RMAN cataloging is enabled, the RMAN tag is automatically generated by SnapCenter to identify the backups. To verify the SnapCenter backup details that are cataloged with RMAN, connect to the RMAN prompt and then enter the following commands:

```
Rman> list datafilecopy all
Rman> list copy of archivelog all
```

The data file backups that are cataloged with RMAN are identified by the unique tag `SCO_<DBname>` as a prefix.

- **Resource croup backups.** If you have multiple databases to be backed up in a short window, consider grouping them in a resource group. It's the same as the protect workflow for an individual database resource. You can schedule multiple resource groups for backups at the same time but the concurrency limit should be carefully observed. During resource group creation, if you group multiple databases in the same host that shares the same volume or LUNs for a backup, you benefit from the Snapshot consolidation feature, which means that one Snapshot copy is taken for all databases instead of multiple Snapshot copies for each database. This also reduces the overall storage overhead and might prevent the system from reaching the Snapshot limit.

Figure 6) Resource group creation.



Note: When you create a common policy and attach it to multiple databases for backup, then it is essential to keep track of databases separately that share the policy because you can't delete the entire policy until you delete backups on all those database.

Additional resources

For more information about how to back up an Oracle database across a hybrid cloud using SnapCenter, see the YouTube demonstration video.

Restore and recovery best practices

The SnapCenter Plug-In for Oracle supports the restore and recovery of an Oracle database. The restore and recovery can be done at full database level or at a granular entities level as low as PDB, PDB tablespaces, legacy 11g tablespace, and control file in a database. The restore process is attempted either by using the storage Snapshot restore mechanism or through Oracle RMAN copy (connect and copy approach). The Snapshot restore process uses the ONTAP SFSR/single-file restore (SFR) technology, which is significantly faster than the Oracle RMAN connect and copy approach.

Here are the cases where restore uses the connect and copy approach rather than Snapshot restore:

- If critical files such as spfile and passwd files with an ASM disk group/LVM that shares along with data files are considered as nonoverridable files.
- If SPL is not installed or SPL is down on the remote node in the case of a RAC database.
- If there are any structural changes to ASM disk group/LVM such as addition or removal of disks after a backup is taken.
- If multiple tablespaces share the file system or disk group and the user selects only one or a subset of tablespaces.
- If the LUN path and LUN serial number change for the ASM disk group after a backup is taken. Can be overridden by using the force-in-place option.
- If there are nested mount points and the user selects a tablespace in a child file system.
- If some other file system is mounted inside the file system requested for restore.
- If there are multiple LVs and the user selects a tablespace residing on one of the LVs.
- In conflicting restore modes such as:
  - Nested mount points and conflicting restore modes: parent– connect and copy; child– in-place restore. Both use connect and copy restore mode.

  - In Nested mount points scenario–if the child mount point is not part of restore scope but parent the mount point is part of restore scope.
  - Multiple file systems in a single volume group and one file system use connect and copy; but if another uses in-place restore, then connect and copy is chosen for all file systems in that volume group.
- If there are any structural changes to the volume group such as addition or removal of LVs after a backup is taken. Can be overridden by using the force-in-place option.
- If a restore on RAC scenario for RDM/VMDK, VMDK residing on NFS/VMFS datastores goes for connect and copy.
- In the case of a file system on VMDK (VMFS datastore), it always uses VMware storage vMotion to copy VMDK from the cloned VMFS datastore to the actual datastore.
- In Oracle RAC setup, on any of the peer nodes if the ASM instance or the cluster instance is not running or if the peer node is down or made offline as standby.
- If new nodes are added to the Oracle RAC and SnapCenter Server is not aware of the newly added nodes
- If RAC one node restore would be always connect and copy .

After the restore activity is complete, you must recover the databases to a specific point-in-time (PiT), system change number (SCN), or the latest log present in the active file system. When recovering to an SCN or a time, SnapCenter checks for the archive logs present in the archive log or FRA destination and applies it for recovery.

Force in-place restore flag in restore wizard

The following use cases can override the connect and copy approach when force-in place restore flag is set in the restore workflow. It is at the risk of the customer to decide whether to enable this or not knowing the implications of enabling this option.

- No new non-database files are added after a backup (foreign file check)—this is applicable in SAN, ASM on SAN, and ASM on NFS layouts.
- No new data files from other databases; Oracle files are sharing mount point/file system (foreign file check), this is applicable in SAN and NFS (non-ASM Layouts).
- No addition, deletion, or recreation of LUNs to LVM disk group (LVM disk group structural change check).

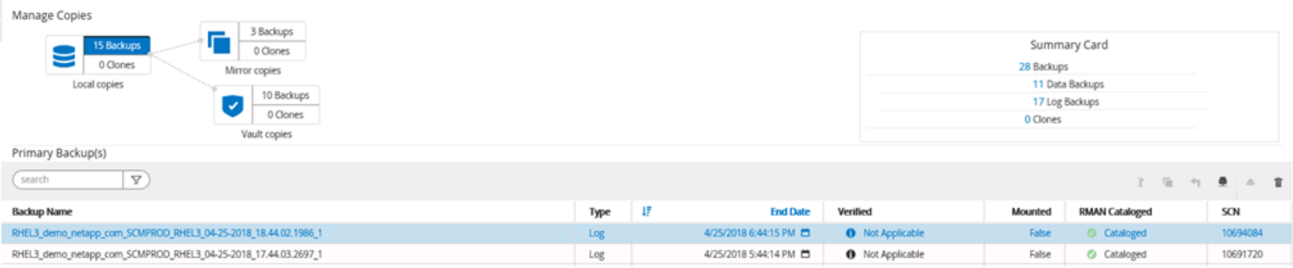
Archive log management for replaying multiple log backups

Sometimes you might require more logs to be applied for consistent recovery or have to roll forward to a time that is beyond the scope of the full backup (data+log). In such cases, you must mount the cataloged log backup on the Oracle host prior to the restore operation and pass that location as an external log location in the restore recovery wizard. Failing to mount the required log backups might cause the entire recovery operation to fail. During the mount operation of a given backup, SnapCenter fires a FlexClone volume at the storage layer and mounts the FlexClone volume/LUN to the host.

To optimize the recovery time, pass multiple log backup destinations (the log backup that was mounted on the Oracle host) in the recovery wizard in ascending order of time, from oldest to newest. When the restore operation is complete, unmount the log backup.

To mount the log backup and pass the mounted destination by using the recovery wizard, follow these steps.

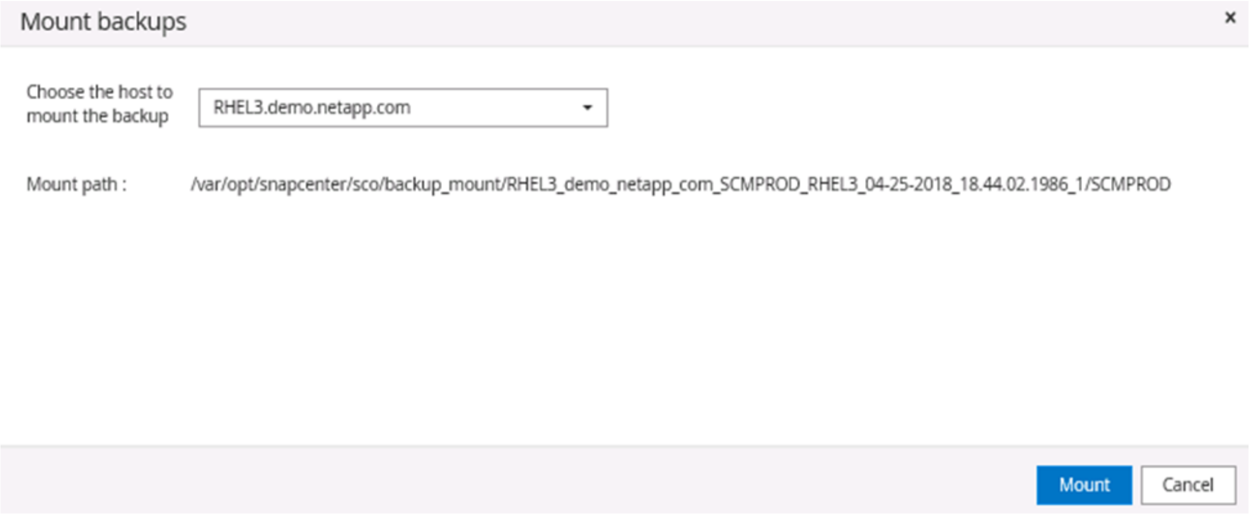
1. Select the latest log backup and click the mount icon.



Backup Name	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_18.44.02.1986_1	Log	4/25/2018 6:44:15 PM	Not Applicable	False	Cataloged	10694084
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_17.44.03.2697_1	Log	4/25/2018 5:44:14 PM	Not Applicable	False	Cataloged	10691720

2. In the Mount wizard, select the host and click Mount.

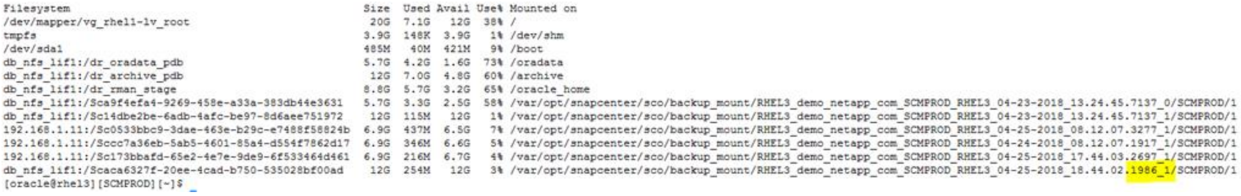
   If you are mounting from a secondary storage location, select the vault or mirror destination.



Choose the host to mount the backup: RHEL3.demo.netapp.com

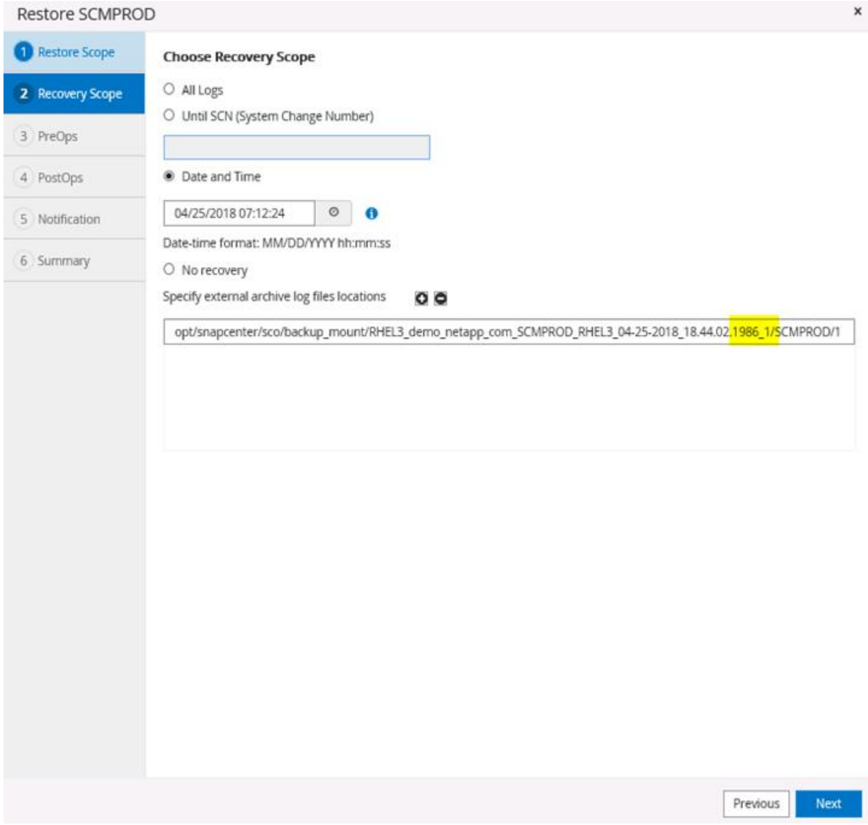
Mount path : /var/opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_18.44.02.1986_1/SCMPROD

3. To check for the mounted log backup, use the `df -h` command on the Oracle host.



```
Filesystem                                          Size  Used Avail Use% Mounted on
/dev/mapper/vg_rhel1-lv_root                         20G  7.1G   12G  38% /
tmpfs                                               3.9G  148K  3.9G   1% /dev/shm
/dev/sda1                                           485M   40M  421M   9% /boot
db_nfs_lif1:/dr_oradata_pdb                         5.7G  4.2G  1.6G  73% /oradata
db_nfs_lif1:/dr_archive_pdb                          12G  7.0G  4.8G  60% /archive
db_nfs_lif1:/dr_rman_stage                          8.8G  5.7G  3.2G  65% /oracle_home
db_nfs_lif1:/Sca9f4efa4-9269-458e-a33a-383db44e3631  5.7G  3.3G  2.5G  58% /var/opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_13.24.45.7137_0/SCMPROD/1
db_nfs_lif1:/Sc14dbe2be-6adb-4afc-be97-8d6aee751972   12G  115M   12G   1% /var/opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_13.24.45.7137_1/SCMPROD/1
192.168.1.11:/Sc0533bbc9-3dae-463e-b29c-e7488f58824b 6.9G  437M  6.5G   7% /var/opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_08.12.07.3277_1/SCMPROD/1
192.168.1.11:/Sccc7a36eb-5ab5-4601-85a4-d554f7862d17 6.9G  346M  6.6G   5% /var/opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-24-2018_08.12.07.1917_1/SCMPROD/1
192.168.1.11:/Sc173bbafd-65e2-4e7e-9de9-6f533464d461 6.9G  216M  6.7G   4% /var/opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_17.44.03.2697_1/SCMPROD/1
db_nfs_lif1:/Scaca6327f-20ee-4cad-b750-535028bf00ad   12G  254M   12G   3% /var/opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_18.44.02.1986_1/SCMPROD/1
[oracle@rhel3][SCMPROD][~]$ _
```

4. Pass this mounted log location in the external archive log files location of the Recovery wizard.



Restore SCMPROD

1 Restore Scope
2 Recovery Scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Choose Recovery Scope

○ All Logs

○ Until SCN (System Change Number)

● Date and Time

04/25/2018 07:12:24

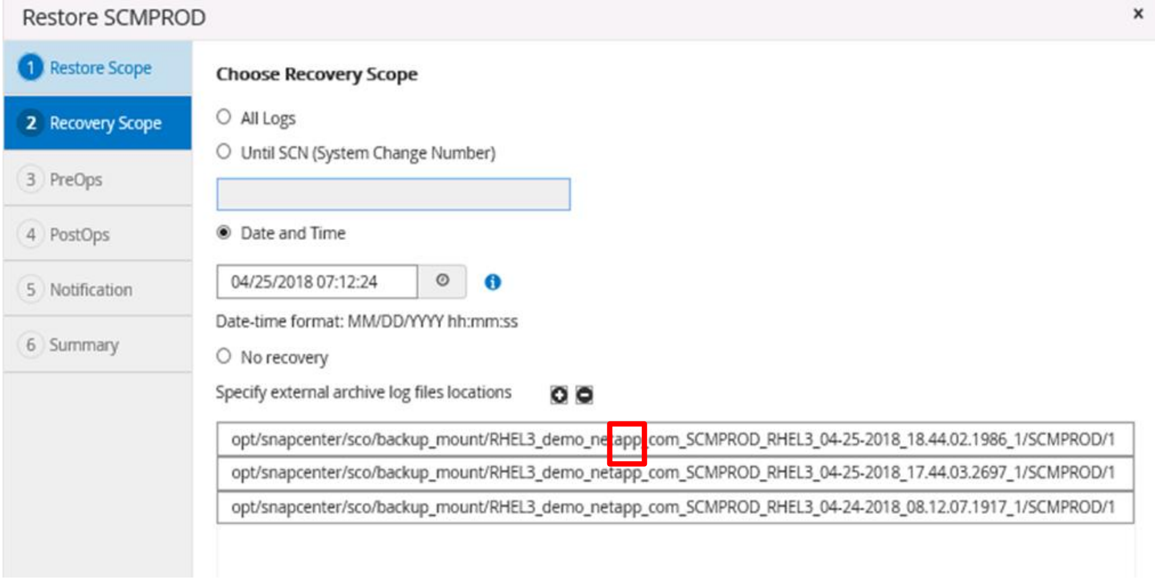
Date-time format: MM/DD/YYYY hh:mm:ss

○ No recovery

Specify external archive log files locations

opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_18.44.02.1986_1/SCMPROD/1

5. If you want multiple logs to be replayed for recovery, mount all of those log backups to the Oracle host and click the plus symbol to pass all these locations in the similar way.



Restore SCMPROD

1 Restore Scope
2 Recovery Scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Choose Recovery Scope

○ All Logs

○ Until SCN (System Change Number)

● Date and Time

04/25/2018 07:12:24

Date-time format: MM/DD/YYYY hh:mm:ss

○ No recovery

Specify external archive log files locations

opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_18.44.02.1986_1/SCMPROD/1
opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_17.44.03.2697_1/SCMPROD/1
opt/snapcenter/sco/backup_mount/RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-24-2018_08.12.07.1917_1/SCMPROD/1

6. To specify the external archive log location based on FRA and non-FRA layouts, use the following formats:

   – For a non-ASM file system, if the archive log destination is not configured on FRA, use the format `/mounted_archive_log/dbname/arch_dest`. Stop with the directory and do not specify the archive log file name.

- For a non-ASM file system, if the archive log destination is configured on FRA, use the format `/mounted_archive_log/dbname/archivelog`. Notice the directories in the date format `YYYY_MM_DD` that contain the list of archive log files for the respective date in this directory.
- For an ASM file system, if the archive log destination is configured on FRA, use the disk group format `+ <Mounted_Archivelog_diskgroup_name>`. Do not specify any other directories or files under this disk group name.

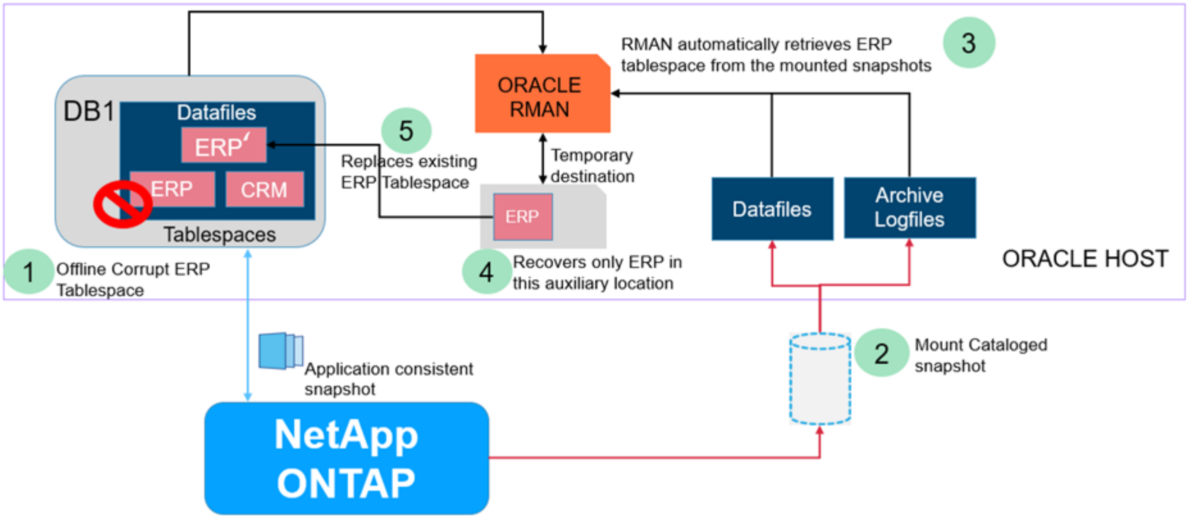
7. For NFS layout, you should pass the external archive log location in ascending order of the file or time; that is, in the order of the logs that the database needs for recovery. If not passed in the correct order, recovery might take a little longer than usual.

   Note: You can do all the supported SnapCenter recovery operations in RMAN by cataloging the Snapshot copies with Oracle RMAN. You can catalog the metadata to target control file or external RMAN catalog. The external catalog file settings can be edited in the database settings in the SnapCenter topology page for a given database.

Important considerations

- In the RAC restore use case, you must manually bring up the other RAC nodes after a successful restore on one of the nodes.
- Selecting or deselecting a control file for restores is crucial during the restore operation. If tablespaces or data files are added to or deleted from the database after the backup, and if control files are not selected for restore, then recovery might fail due to inconsistency in the current control file and backup control file. The best practice is to take a backup whenever there is a change in the database architecture.
- You can do a more granular restore and recovery by using the SnapCenter backups that are cataloged with RMAN. To explore various restore workflows, see the appendix.
- With SnapCenter 4.4, you can now perform a PITR- or SCN-based recovery for PDB or PDB tablespace. Instead of doing it manually through RMAN (as described in the Appendix C), you can simply use SnapCenter, which has stitched all the manual steps, as shown in Figure 7. Make sure the control file is not selected for restore.

Figure 7) Detailed workflow of tablespace PiT restore and recovery.


DB1
Datafiles
ERP′
ERP
CRM
Tablespaces
1
Offline Corrupt ERP Tablespace
5
Replaces existing ERP Tablespace
ORACLE RMAN
Temporary destination
ERP
4
Recovers only ERP in this auxiliary location
3
RMAN automatically retrieves ERP tablespace from the mounted snapshots
Datafiles
Archive Logfiles
ORACLE HOST
Application consistent snapshot
NetApp ONTAP
2
Mount Cataloged snapshot

Additional resources

For more information about:

- How to perform a quick and easy restore of Oracle multitenant database using NetApp SnapCenter, see the following YouTube demonstration video.
- How to perform a tablespace PiT recovery using cataloged Snapshot copies, see the following YouTube demonstration video.

Oracle database clone and refresh best practices

You can use SnapCenter to clone a database by using the snapshot of the database. The clone operation creates a copy of the database data files and creates new online redo log files, control files, and archive log destination. The clone database can also be recovered to a specified time, SCN, or Until Cancel.

Before you perform a clone operation, review the following prerequisites and best practices:

- If you want to customize the location of a control file or redo log file paths, verify that you have provisioned the required file system or ASM disk group.

  By default, redo log and control files of the cloned database are created on the ASM disk group or the file system provisioned by SnapCenter for the data files of the clone database.
- A clone can be created on the same host as that of the source database. When creating the clone on an alternate host, confirm that the alternate host meets the following requirements:
  - SnapCenter Plug-In for Oracle database is installed on the alternate host.
  - The clone host is able to discover LUNs from primary or secondary storage. For example, if you are cloning from primary storage or secondary (vault or mirror) storage to an alternate host, make sure that an iSCSI session is established between the primary or secondary storage and the alternate host, or that it is zoned properly for FC.
  - The Oracle home version is the same as that of the source database host.
  - The operating system distribution and version are the same as those of the source database host.

    If you want to override the clone to a different operating system version within the same Linux distribution, specify the parameter as follows:

    a. Set the parameter `ALLOW_CLONE_OS_MISMATCH=TRUE` in the `/var/opt/snapcenter/sco/etc/sco.properties` file.

    b. Restart the plug-in service `/opt/NetApp/snapcenter/spl/bin/spl restart`.
- If the source database is an ASM database:
  - Make sure that the ASM instance is running on the host where the clone is being performed.
  - If you want to place archive log files of the cloned database in a dedicated ASM disk group, make sure that the ASM disk group is provisioned prior to the clone operation.
  - The name of the data disk group can be defined, but you should verify that the name is not used by any other ASM disk group on the host where the clone is being performed.
  - To clone a backup of a 12c R1 database, set the value of `exclude_seed_cdb_view` to `FALSE` in the source database parameter file to retrieve seed PDB-related information.

  The seed PDB is a system-supplied template that the container database (CDB) can use to create PDBs. The seed PDB is named `PDB$SEED`. For information about `PDB$SEED`, see the Oracle Doc ID 1940806.1.
- You can also perform a clone operation from Data Guard and Active Data Guard Standby databases. Remember to follow back-up best practices for Data Guard and Active Data Guard configurations outlined in SnapCenter Resource Group and Policies Best Practices.

Cloning a multitenant pluggable database

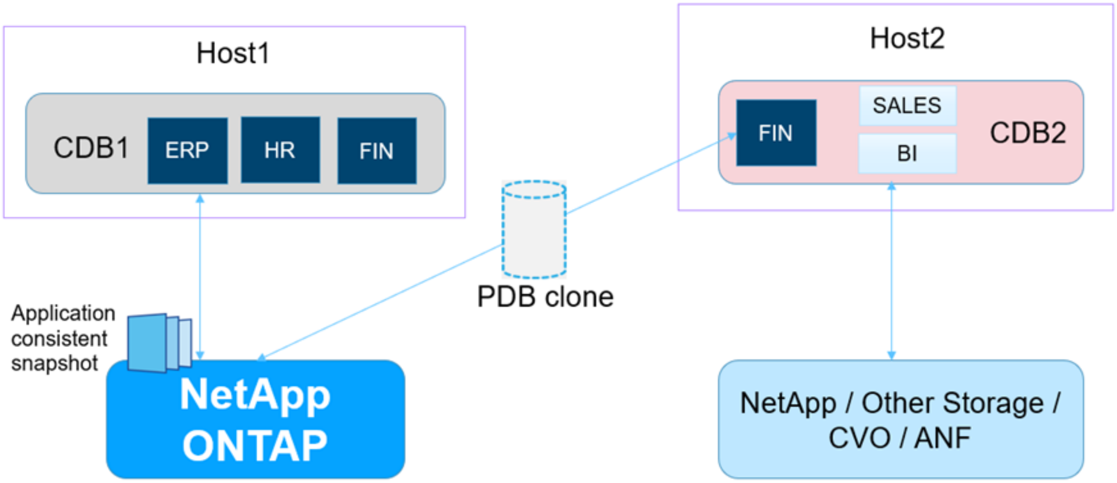
To understand more about Oracle multitenancy best practices , refer to TR 4876: Oracle Multitenancy with ONTAP Solution and Deployment Best Practices.

Oracle offers two different methods to clone Oracle PDBs. One method is still dependent on the streaming copy-based approach and uses database link to refresh PDBs to alternate CDB in a different host. The other method is based on copy-on write (COW) at the file-system level, which is presently applicable only for DNFS layout and is limited within the same host, and the source database must be read only.

You can overcome these limitations by using NetApp SnapCenter 4.4. You can easily clone a PDB within a CDB to the same or different CDB on a different host by using SnapCenter backups, as shown in Figure 8. At the time this document was written, NetApp was the first storage vendor to support this big clone feature.

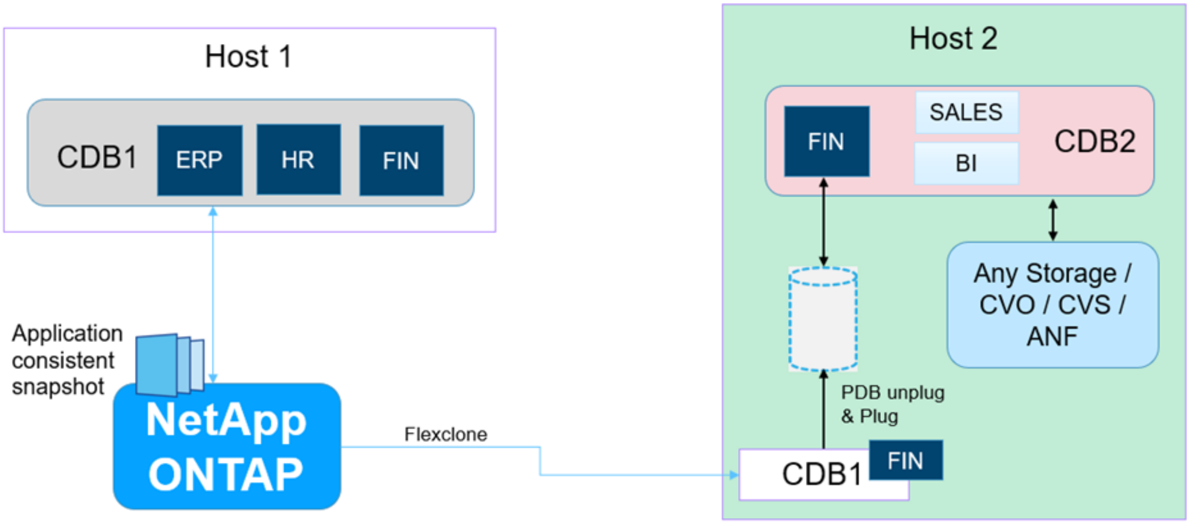
Ensure the CDB versions and compatibility versions are same at the target. If the CDB version is higher or lower than the source, then it can fail.

Figure 8) PDB clone.


Host1
CDB1
ERP
HR
FIN
Application consistent snapshot
NetApp ONTAP
PDB clone
Host2
FIN
SALES
BI
CDB2
NetApp / Other Storage / CVO / ANF

The internal workflows within this PDB clone is fully orchestrated and managed by stitching the multiple steps listed in Figure 9. For a how-to demo, see the additional resources.

Figure 9) Detailed PDB clone workflow from one CDB to another CDB.



The storage associated with the PDB clone is efficiently determined and attached to host2 without consuming the storage for the entire CDB.

Clone life cycle management and clone as a service

SnapCenter supports clone life cycle management (CLM) for Oracle database through the Linux CLI. This feature is slightly different from the typical CLM feature supported by SnapCenter Plug-in for SQL Server. The syntax for the `refresh-SmClone` is captured in Linux Commandlet Guide. The CLM feature addresses the following workflows :

1. Creates an on-demand backup using a specified policy and resource group.
2. Deletes an existing clone (if any) with the same database secure identifier (SID) specified in the clone specification file (XML file).
3. Creates a new clone database with the database SID and the other information specified in the clone specification XML file using the on-demand backup taken in step 1. If clone delete couldn't successfully delete the resource in step 2, and if a new clones initiates with the same database SID, then this operation might fail.

   You must generate a clone specification file for this type of automation. For information about how to generate a spec file for clones, see the section titled "SCO CLI and Workflow Automation." You can customize entries for each clones. To reuse these spec files for subsequent refreshes with the same settings, NetApp recommends that you pass the backup name and the `refresh-SmClone` syntax.

```
# sccli Refresh-SmClone
- OracleCloneSpecificationFile '/var/opt/snapcenter/sco/clone_specs/oracle_clonespec_dgp_CLSID1_2
018-06-04_02.35.05.605.xml'
-PolicyName polSecondary
-CloneDatabaseSID sid2
- BackupName scspr0473539001_gdl_englab_netapp_com_dgp_scspr0473539001_06-15-
2018_01.45.02.7306_0
-ResourceGroupName rg1
-SecondaryUpdateWaitTimeout 20
```

You can even automate the clones at scale with multiple databases by using the customized script provided in the section titled, "SCO CLI and Workflow Automation."

Important considerations

- In the event of a load-sharing (LS) mirror, the clone operation might fail if LS mirror updates take too long on the storage system. The workaround is to include the following parameters and specify the value in the `<appSettings>` section of the `SMCoreServiceHost.exe` configuration file, located under SMCore in SnapCenter Server. Then restart the SnapCenter SMCore service.

```
 <add key="lsmsleep" value="300000">
```

The value 300,000 (in ms) results in a 300-second wait.

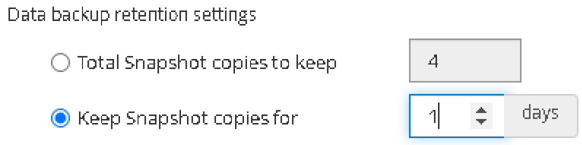
- The clone from a RAC instance is always non-RAC. If you want to convert it to RAC , follow the steps described in Appendix F.
- When a clone from SnapVault secondary for FC SAN/ASM configuration fails with `Error executing SQL "ALTER DATABASE OPEN RESETLOGS` within `2100 seconds against Oracle database`, the workaround is to run the following commands on the Linux node that is hosting the clone:

```
cd /opt/NetApp/snapcenter/spl/bin/sccli or /spl
./sccli Open-SmConnection
./sccli Set-SmConfigSettings -ConfigSettingsType Plugin -PluginCode SCO -ConfigSettings
"KEY=ORACLE_SQL_QUERY_TIMEOUT,VALUE=10800"
./sccli Set-SmConfigSettings -ConfigSettingsType Plugin -PluginCode SCO -ConfigSettings
"KEY=ORACLE_PLUGIN_SQL_QUERY_TIMEOUT,VALUE=10800
```

Restart the SPL process to reflect the change.

```
./spl restart   (absolute path)
```

- If you have two clones (CL1 and CL2) that were created from the same database (RTPPRD) using SnapCenter with a backup retention, as mentioned below.



Data backup retention settings

○ Total Snapshot copies to keep 4

● Keep Snapshot copies for 1 days

There might be instances where you want to keep the clone (CL1) for more time (for example, two days) with its associated backup; however, when you want to refresh clone CL2, it fails with the following error. This occurs because the refresh process tries to apply a retention algorithm for the backups and attempts to delete the backup that is still being used by clone CL1. Because the backup was older than one day (the retention period set above), there is a failure in `Refresh-SmClone` and the target clone isn't created.

```
INFO: Using localhost XXXXX' as default host for clone operation.
INFO: Backing up the resource cid-cluster\ RTPPRD
ERROR: Job Warning: ^M
Failed on 'CIDXXXXX2':^M
Activity 'Registering Backup and Applying Retention' failed with error: Retention : Failed to
delete backup as there are clone(s) created from this backup. Please delete clone(s) -
RTPPRD__clone__XXXX (Source Object - RTPPRD, Clone Object - RTPDEV) before deleting backup.
INFO: A connection session with the SnapCenter was closed.
```

In this example, is better to temporarily increase the retention of backups in the backup policy. If you have a higher retention (for example, three days) with more Snapshot copies, it can still skip the existing Snapshot copy blocked by the clone and attempts to remove the subsequent Snapshot copy.

Additional resources

For more information about using SnapCenter, see the following additional resources:

- To clone an Oracle database to an alternate host running in a public cloud (AWS, Azure), see the following YouTube demonstration video.

- To clone an Oracle multitenant PDB from CDB to another CDB running in a different host using storage Snapshot technology, see the following YouTube demonstration video.

General Oracle Plug-in best practices

Regardless of whether it's hosted on multiple storage clusters, SVMs, or volumes, SnapCenter always takes a consistency group Snapshot during a backup of the databases. In SnapCenter, while grouping multiple databases in a single resource group for parallel backup, the scope of the consistency group is at the application (ASM disk group) or file system (LVM disk group) entities (regardless of the number of databases [of a single host] in a resource group).

For example:

There are two databases on a host. Each of them resides on a dedicated ASM disk group and they are part of single resource group.

```
Db1: +DATA1    ==== First CG snapshot is cut for all LUNs which is part of DATA1.
Db2: +DATA2    ==== Second CG snapshot is cut for all LUNs which is part of DATA2
```

1. After the plug-in is installed and configured on the Oracle host, the databases should appear on the resources screen. If the database is a RAC database, it is a best practice to enable the preferred nodes for backup in the Configure Database wizard. This configuration serves two purposes: to handle host/instance failures and to dedicate the backups to a separate node to isolate the load.
2. If you have a RAC or RAC One Node database, always select the option to add the cluster nodes in Add Host for RAC Awareness and verify that the plug-ins are pushed on all the cluster nodes or manually installed on them.
3. If archive logs have been deleted outside of SnapCenter or RMAN, enable the parameter `ENABLE_CROSSCHECK=true` in the `sco.properties` file to avoid unexpected delays in searching for the stale archive log entries during backup. The `sco.properties` file is located in `/var/opt/snapcenter/sco/etc`.
4. The retention logic for backups is verified only at the end of each backup job. If any Snapshot (backup) copy is locked by a FlexClone volume (due to clone or mount operations), the retention skips the current Snapshot copy that is locked and moves on to the next one. This might be a limitation in the case of `sm-clone refresh` job when a backup is locked by the clone and when the retention algorithm is applied, the subsequent backup and clone jobs fail.
5. When a large amount of data is being transferred, SnapVault replication of backups might time out. Therefore you should include the parameters listed below with higher values and specify the values in the `<appSettings>` section of the `SMCoreServiceHost.exe` config file located under `C:\Program Files\NetApp\SMCore` in the SnapCenter Server.

   Restart the SnapCenter SMCore service (timeout values are in milliseconds.)

```
<appSettings>
<add key="SnapmirrorRetry" value="288"/>
<add key="SnapmirrorTimeout" value="300000"/>
<add key="SnapshotCheckRetry" value="288" />
<add key="SnapshotCheckTimeout" value="300000" />
</appSettings>
```

6. The IMT indicates that SnapCenter plugin for Oracle (SCO) won't work for Oracle Transparent Data Encryption (TDE)/Oracle Advanced Security. It is meant for scenarios where no auto-login mode was enabled. SCO backup and restore should work with Oracle TDE/Oracle Advanced Security. For SCO clone, as long as wallet/key is available and managed with auto-login, it should work. In the event of cloning to a new host , you should copy wallet (key files) under `/etc/ORACLE/WALLET/$ORACLE_SID` from the source database to the cloned database.
7. SnapCenter allows you to protect databases on NVE-enabled volumes.

8. SnapCenter offline backups can be used as alternative backout source for database migration or upgradation. In the event of a failure, you can revert back to the old state.

SCO CLI and workflow automation

Perform a silent installation of the plug-in

To perform a silent installation of the plug-in, rub the following command:

```
snapcenter_linux_host_plugin.bin -i silent -DPORT=8145 -DSERVER_IP=xxxx-DSERVER_PORT=8146
```

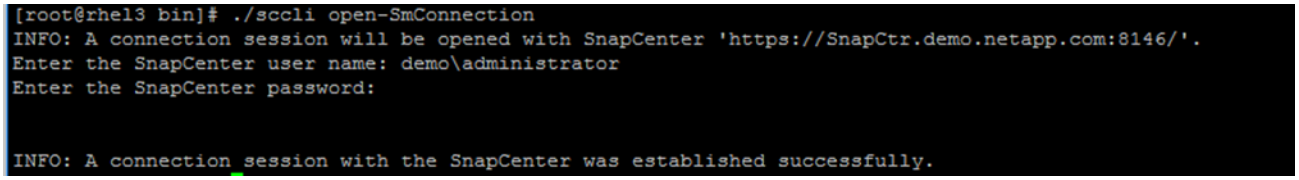
To register the Linux host with the SnapCenter Server, run the `add-smHost` cmdlet in PowerShell. For the syntax, see Cmdlet Reference Guide for Windows.

Back up by using the SCO CLI

To perform a backup using the CLI, use the SCO CLI located in the following directory:

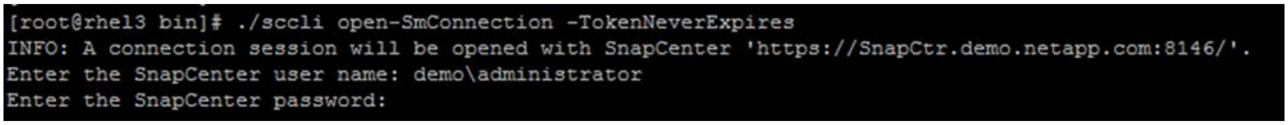
```
/opt/NetApp/SnapCenter/spl/bin.
```

Note: Open the connection to SnapCenter Server running on a Windows Server:



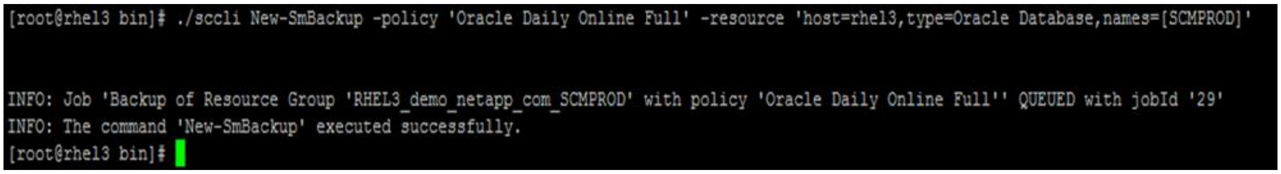
```
[root@rhel3 bin]# ./sccli open-SmConnection
INFO: A connection session will be opened with SnapCenter 'https://SnapCtr.demo.netapp.com:8146/'.
Enter the SnapCenter user name: demo\administrator
Enter the SnapCenter password:


INFO: A connection session with the SnapCenter was established successfully.
```

If you want to keep the connection open until reboot of the server, pass an additional parameter `TokenNeverExpires` to disable token expiry. For security reasons, NetApp does not recommend keeping the token open.



```
[root@rhel3 bin]# ./sccli open-SmConnection -TokenNeverExpires
INFO: A connection session will be opened with SnapCenter 'https://SnapCtr.demo.netapp.com:8146/'.
Enter the SnapCenter user name: demo\administrator
Enter the SnapCenter password:
```

Note: After creating backup policies and enabling protection for a resource or resource group, run the following command to back up the entire database (data file and archive log).



```
[root@rhel3 bin]# ./sccli New-SmBackup -policy 'Oracle Daily Online Full' -resource 'host=rhel3,type=Oracle Database,names=[SCMPROD]'


INFO: Job 'Backup of Resource Group 'RHEL3_demo_netapp_com_SCMPROD' with policy 'Oracle Daily Online Full'' QUEUED with jobId '29'
INFO: The command 'New-SmBackup' executed successfully.
[root@rhel3 bin]#
```

Note: You can verify the additional parameters and syntaxes by using `-help`.

```
./sccli -help
./sccli New-SmBackup -help
```

Perform a clone operation by using the CLI

Create an Oracle database clone specification from a specified backup.

The command automatically creates an Oracle database clone specification file for the specified source database and its backup. You must also enter a clone database SID so that the specification file created has the automatically generated values for the clone database that you are creating. You can also specify the recovery options, the host where the clone operation is to be performed, prescripts, postscripts, and other details.

```
sccli New-SmOracleCloneSpecification -AppObjectId [-BackupName | -CloneLastBackup ] -
CloneDatabaseSID [-IncludeSecondaryDetails] [-SecondaryStorageType ] [- SetConsoleOutputWidth]
```

Sample syntax:

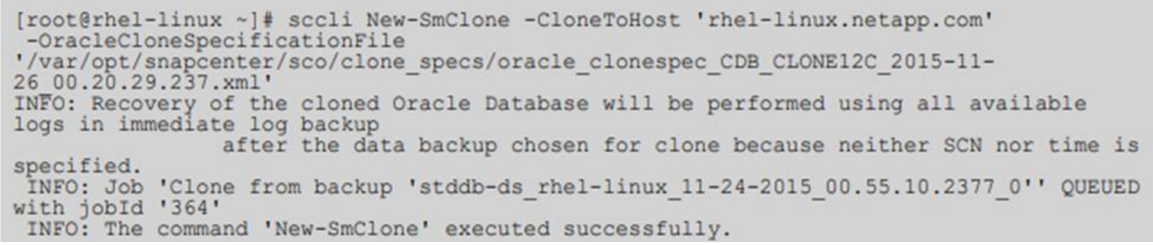
```
[root@rhel-linux ~]# sccli New-SmOracleCloneSpecification -AppObjectId
'rhellinux.netapp.com\STDDB' -CloneLastBackup 2 -CloneDatabaseSID 'CDBCLONE'

INFO: You have chosen to generate clone specification using last backup number '2' having backup
name 'federated-ds_rhel-linux_10-25-2015_22.30.30.4523_0'.

INFO: Oracle clone specification file
'/var/opt/SnapCenter/sco/clone_specs/oracle_clonespec_CDB_CDBCLONE_2015-10- 25_23.59.12.317.xml'
got created successfully.

INFO: The command 'New-SmOracleCloneSpecification' executed successfully..
```

Initiate a clone operation from an existing backup.

This command initiates a clone operation. You must also enter an Oracle clone specification file path for the clone operation.

By default, the archive log destination file for the clone database is automatically populated at `$ORACLE_HOME/CLONE_SIDs`.

Sample syntax:



```
[root@rhel-linux ~]# sccli New-SmClone -CloneToHost 'rhel-linux.netapp.com'
 -OracleCloneSpecificationFile
'/var/opt/snapcenter/sco/clone_specs/oracle_clonespec_CDB_CLONE12C_2015-11-
26_00.20.29.237.xml'
INFO: Recovery of the cloned Oracle Database will be performed using all available
logs in immediate log backup
                after the data backup chosen for clone because neither SCN nor time is
specified.
 INFO: Job 'Clone from backup 'stddb-ds_rhel-linux_11-24-2015_00.55.10.2377_0'' QUEUED
with jobId '364'
 INFO: The command 'New-SmClone' executed successfully.
```

For more information about the CLI commands, see the Command Reference Guide.

Clone as a service

The following sample customized utility script can be leveraged for executing multiple clones from the same or multiple databases by using the CLI.

Note: This example is not supported by NetApp and should not be distributed, modified, or sold without written consent from NetApp. This script must be tested rigorously in a proof-of-concept (POC) lab before being moved or executed in production.

```
#!/bin/bash
#
# Copyright (c) 2018 NetApp, Inc., All Rights Reserved
#   Any use, modification, or distribution is prohibited
#   without prior written consent from NetApp, Inc.
# Test the script in POC lab before deploying in production
# This is just a utility script which is not backed by NetApp support
# Author: Vasantha Prabhu, Ebin Kadavy
# Version: 1.0
#
```

```
if [ $# -lt 8 ]; then
    echo "Usage: -Destinations HostName1:CloneSID1,HostName2:CloneSID2 -
OracleCloneSpecificationFile spec1,spec2 -SourceAppObjectId sourceappobjectid -PolicyName policy"
    echo "Optional arguments: -ResourceGroupName rg1,rg2 -SecondaryUpdateWaitTimeout <timeout> -
WaitToTriggerClone <wait time> "
    echo "Optional arguments: -OracleSkipRecovery -OracleUntilCancel -OracleUntilScn scnnumber -
OracleUntilTime 'yyyy-MM-dd HH:mm:ss' "
    echo "Optional arguments: -AlternateArchiveLogPaths 'location1, location2, ..., locationN' -
PreScriptPath <script path> -PreScriptArguments <arg1,arg2 ... argN> "
    echo "Optional arguments: -PostScriptPath <script path> -PostScriptArguments <arg1,arg2 ...
argN> -ScriptTimeout <timeout> "
    echo "Optional arguments: -EnableEmail -EmailTo <email address> -EmailFrom <email address> -
EmailSubject <subject> -EmailPreference <ALWAYS | ON_ERROR | ON_ERROR_OR_WARNING | NEVER> "
    echo "Optional arguments: -EnableEmailAttachment -SkipNIDCreation "
    exit 1;
fi
sourceappobjectid_option=0
destinations_option=0
clonespecs_option=0
policy_option=0
resourcegroupname_option=0
optional_params=""
resourcegroup_params=""
waittotriggerclone_option=1

for arg in "$@"; do
  case "$arg" in
        "-Destinations")
            destinations=$2
            echo "value is $destinations"
            IFS=’,’ read -ra destinations_array <<< "$destinations"
            destinations_option=1
            ;;
        "-OracleCloneSpecificationFile")
            clonespecs=$2
            echo "value is $clonespecs"
            IFS=’,’ read -ra clonespecs_array <<< "$clonespecs"
            clonespecs_option=1
            ;;
        "-SourceAppObjectId")
            sourceappobjectid_option=1
            sourceappobjectid=$2
            echo "value is $sourceappobjectid"
            IFS=’,’ read -ra sourceappobjectid_array <<< "$sourceappobjectid"
            ;;
        "-PolicyName")
            policy=$2
            echo "value is $policy"
            IFS=’,’ read -ra policy_array <<< "$policy"
            policy_option=1
            ;;
        "-ResourceGroupName")
            resourcegroupname=$2
            echo "value is $resourcegroupname"
            IFS=’,’ read -ra resourcegroupname_array <<< "$resourcegroupname"
            resourcegroupname_option=1
            ;;
        "-SecondaryUpdateWaitTimeout")
            optional_params+=" -SecondaryUpdateWaitTimeout $2 "
            ;;
        "-WaitToTriggerClone")
            # Do not add to optional params, as if it is single db, we can trigger N-1 clones in
parallel
            waittotriggerclone_option=$2
            ;;
        "-OracleSkipRecovery")
            optional_params+=" -OracleSkipRecovery "
            ;;
        "-OracleUntilCancel")
            optional_params+=" -OracleUntilCancel "
            ;;
        "-OracleUntilScn")
            optional_params+=" -OracleUntilScn $2 "
            ;;
        "-OracleUntilTime")
            optional_params+=" -OracleUntilTime $2 "
            ;;
        "-AlternateArchiveLogPaths")
            optional_params+=" -AlternateArchiveLogPaths $2 "
            ;;
        "-PreScriptPath")
            optional_params+=" -PreScriptPath $2 "
            ;;
        "-PreScriptArguments")
            optional_params+=" -PreScriptArguments $2 "
            ;;
        "-PostScriptPath")
            optional_params+=" -PostScriptPath $2 "
            ;;
        "-PostScriptArguments")
            optional_params+=" -PostScriptArguments $2 "
            ;;
        "-ScriptTimeout")
            optional_params+=" -ScriptTimeout $2 "
            ;;
        "-EnableEmail")
            optional_params+=" -EnableEmail "
            ;;
        "-EmailTo")
            optional_params+=" -EmailTo $2 "
            ;;
        "-EmailFrom")
            optional_params+=" -EmailFrom $2 "
            ;;
        "-EmailSubject")
            optional_params+=" -EmailSubject $2 "
            ;;
        "-EmailPreference")
            optional_params+=" -EmailPreference $2 "
            ;;
        "-EnableEmailAttachment")
            optional_params+=" -EnableEmailAttachment "
            ;;
        "-SkipNIDCreation")
            optional_params+=" -SkipNIDCreation "
            ;;
   esac
   shift
done

echo "Optional parameters passed are $optional_params"

#Sanity check total number of destinations must be same as clone specs
if [ ${#destinations_array[@]} -ne ${#clonespecs_array[@]} ]; then
    echo "Mismatch in destinations and clonespec count";
    exit 1;
fi

if [ $sourceappobjectid_option -ne 1 ]; then
    echo "SourceAppObjectId option is not passed";
    exit 1;
fi

if [ $clonespecs_option -ne 1 ]; then
    echo "OracleCloneSpecificationFile option is not passed";
    exit 1;
fi

if [ $destinations_option -ne 1 ]; then
    echo "Destinations option is not passed";
    exit 1;
fi
```

```
if [ $policy_option -ne 1 ]; then
    echo "PolicyName option is not passed";
    exit 1;
fi


if [ ${#sourceappobjectid_array[@]} -eq 1 ]; then
    for (( i=0; i<${#destinations_array[@]}; i++ ));
    do
        IFS=’:’ read -ra clone_destination <<< "${destinations_array[$i]}"
        clonehostname=${clone_destination[0]}
        clonesid=${clone_destination[1]}
        clonespec=${clonespecs_array[$i]}
        if [ $resourcegroupname_option -eq 1 ]; then
            resourcegroup_params=" -resourcegroupname ${resourcegroupname_array[0]}"
        fi
        echo "Obtained $clonehostname $clonesid $clonespec for iteration $i"
        if [ $i -eq 0 ]; then
            sccli Refresh-SmClone -OracleCloneSpecificationFile $clonespec -PolicyName $policy -
CloneToHost $clonehostname -CloneDatabaseSID $clonesid $optional_params $resourcegroup_params -
WaitToTriggerClone $waittotriggerclone_option
            backupname=`sccli get-smbackup -appobjectid $sourceappobjectid -SetConsoleOutputWidth
1000 | grep "Oracle Database Data Backup"  | head -n 1 | cut -d"|" -f 3`
            if [ -z "$backupname" ]; then
                echo "Could not fetch the latest Oracle Database backup"
                exit 1;
            fi
        else
            sccli Refresh-SmClone -OracleCloneSpecificationFile $clonespec -BackupName
$backupname -CloneToHost $clonehostname -CloneDatabaseSID $clonesid -PolicyName $policy -
WaitToTriggerClone 0 &
        fi
    done
else
    for (( i=0; i<${#destinations_array[@]}; i++ ));
    do
        IFS=’:’ read -ra clone_destination <<< "${destinations_array[$i]}"
        clonehostname=${clone_destination[0]}
        clonesid=${clone_destination[1]}
        clonespec=${clonespecs_array[$i]}
        if [ -z "${policy_array[$i]}" ]; then
            policyname=${policy_array[0]}
        else
            policyname=${policy_array[$i]}
        fi
        if [ $resourcegroupname_option -eq 1 ]; then
            if [ -z "${resourcegroupname_array[$i]}" ]; then
                rgname=${resourcegroupname_array[0]}
            else
                rgname=${resourcegroupname_array[$i]}
            fi
            resourcegroup_params=" -resourcegroupname $rgname"
        fi
        echo "Obtained $clonehostname $clonesid $clonespec $policyname $rgname for iteration $i"
        sccli Refresh-SmClone -OracleCloneSpecificationFile $clonespec -PolicyName $policyname -
CloneToHost $clonehostname -CloneDatabaseSID $clonesid $optional_params $resourcegroup_params -
WaitToTriggerClone $waittotriggerclone_option &
    done
fi
```

Although this script can address multiple use cases, there are the two major use cases that are listed here for reference:

- Use case 1: Single database, multiple clones usage:

```
# ./CloneAsService.sh -Destinations galaxy-vm134.gdl.englab.netapp.com:clone10,galaxy-
vm134.gdl.englab.netapp.com:clone11,galaxy-vm134.gdl.englab.netapp.com:clone12 -
OracleCloneSpecificationFile /vasanth/clone10_spec,/vasanth/clone11_spec,/vasanth/clone12_spec -
SourceAppObjectId galaxy-vm134.gdl.englab.netapp.com\\nasdb10 -PolicyName full_backup -
```

```
ResourceGroupName rg1 -EnableEmail -EmailTo xxxx@netapp.com -EmailFrom xxxxx@netapp.com -
EmailSubject CLM -EmailPreference ALWAYS -EnableEmailAttachment -SkipNIDCreation
```

- Use case 2: Multiple database, multiple clones usage:

```
# ./CloneAsService.sh -Destinations galaxy-vm134.gdl.englab.netapp.com:clone10,galaxy-
vm134.gdl.englab.netapp.com:clone11,galaxy-vm134.gdl.englab.netapp.com:clone12 -
OracleCloneSpecificationFile /vasanth/clone10_spec,/vasanth/clone11_spec,/vasanth/clone12_spec -
SourceAppObjectId galaxy-vm134.gdl.englab.netapp.com\\nasdb10, galaxy-vm134.gdl.englab.netapp.com\\nasdb11,
galaxy-vm134.gdl.englab.netapp.com\\nasdb12 -PolicyName full_backup,full_backup1,full_backup2 -
ResourceGroupName rg1,rg2,rg3 -EnableEmail -EmailTo xxxx@netapp.com -EmailFrom xxxxx@netapp.com -
EmailSubject CLM -EmailPreference ALWAYS -EnableEmailAttachment -SkipNIDCreation
```

Appendix A: SnapCenter deployment models for Oracle Database

SnapCenter can deployed in either of three models:

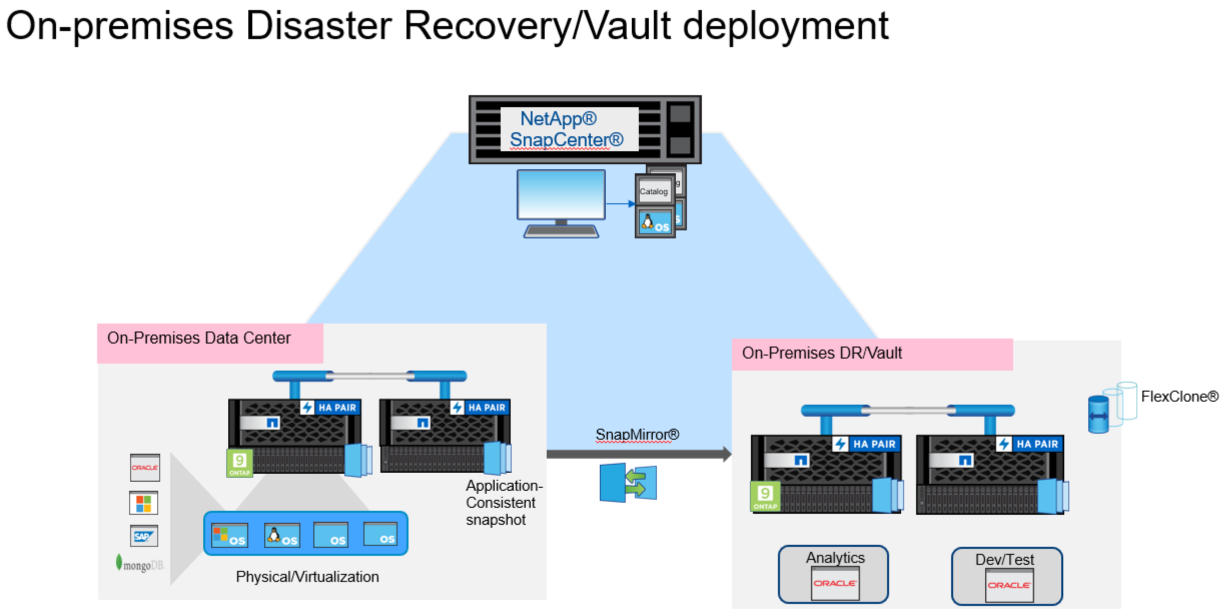
- Private data center/cloud
- Public cloud
- Hybrid cloud

Private data center/cloud

In a private data center/cloud deployment, both the primary and secondary vault or disaster recovery storage Oracle hosts are running on premises. This is the most generic model.

Figure 10 shows a data center/cloud deployment.

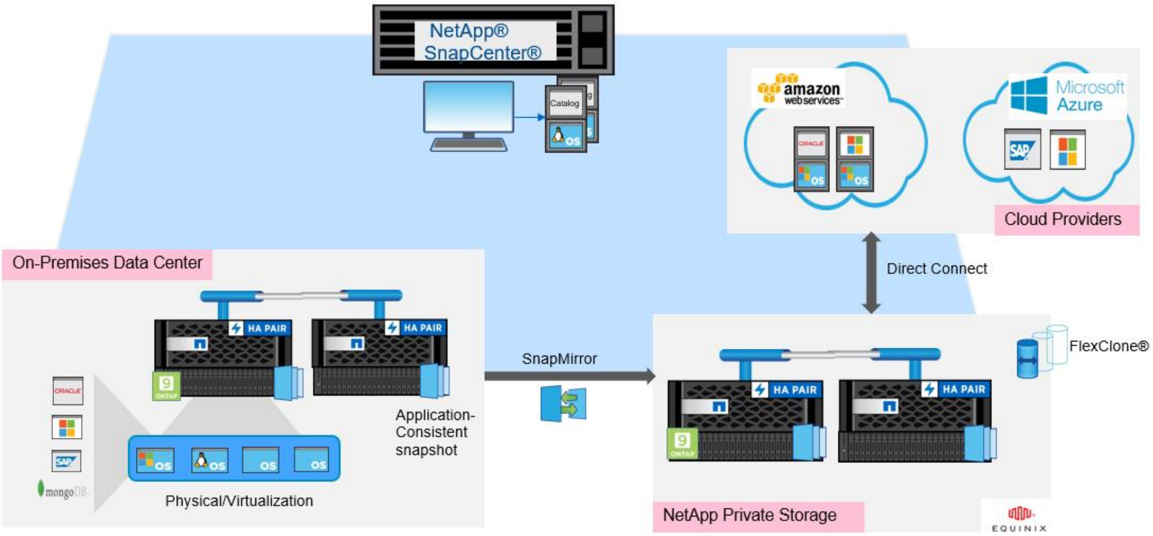
Figure 10) Private data center/cloud deployment.



Hybrid cloud deployment using a collocated data center is also called next-to-cloud deployment using NetApp Private Storage (NPS). In this deployment, the secondary storage is completely running in a private (controlled) environment hosted in a colocated data center, such as Equinix, and the compute is leveraged from the cloud. This is probably the safest model, because the data is in your control. The advantage of this model is that you can switch between different hyperscalar clouds, based on the workload requirements against cost.

Figure 11 shows an NPS deployment.

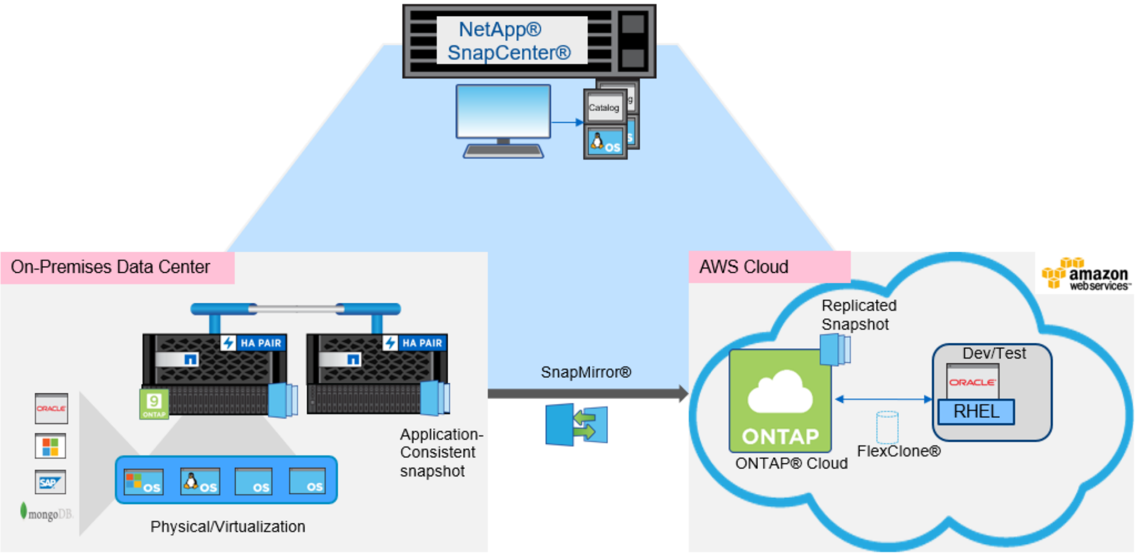
Figure 11) NPS deployment.



Hybrid cloud

Figure 12 shows a typical hybrid cloud deployment. The primary storage is running on premises and secondary storage (vault or disaster recovery) is running on a public cloud (Amazon, Azure, and so on). The ONTAP cloud storage is running on public cloud as a replica destination. This is very a good reference model for dev/test scenarios. You can dynamically spin hosts and host a dev/test whenever required. This model also avoids holding any dedicated infrastructure for secondary disaster recovery or vault in the on-premises data center.

Figure 12) Hybrid cloud deployment



Appendix B: RAC one node and other third-party cluster solutions (active-passive)

RAC One Node and other active-passive cluster solutions work well with SnapCenter, although it is not tailor-made for these configurations such as Oracle RAC. Most of the workflows are like the usual layouts, which are independent of the cluster layouts. However, the scope of migrating the backups during failover of the database to an alternate cluster node is important and involves some manual changes in SnapCenter. Therefore you should follow the guidelines and test all the workflows before moving to production.

RAC One Node layouts

To work with RAC One Node layouts, complete the following steps:

1. Register with all the nodes (Node1, Node2) in the Oracle RAC cluster.
2. Discover the databases on all the nodes.

   The RAC One Node database is discovered as the RAC database on the node (Node1) where it is currently hosted.

   The same database is discovered as a standalone database on all the other RAC nodes (Node2); this is a stale entry that can be ignored.

   Backup, restore, and clone workflows exercised on the initial node (Node1), where the RAC One Node database is active, are successful.
3. When you have migrated the RAC One Node database from Node1 to Node2 and performed a manual resource discovery on both nodes:

   The RAC One Node database is discovered as a RAC database on the node (Node2) where it is currently hosted.

   The same database is discovered as a standalone database on all the other RAC nodes (Node1); this is a stale entry that can be ignored.

   All the backups performed previously on other nodes of RAC One Node are still visible and are valid.

4. When the database is migrated to Node2 from Node1, you must manually configure the preferred host as Node2 in a preferred RAC node.
5. You can exercise restore and clone workflows in the usual way on the active node.
6. Similarly, you can migrate back the RAC One Node database from Node2 to Node1 and perform a manual resource discovery on both nodes. As mentioned in step 4, you must manually configure the preferred host as Node1.

   For other cluster solutions (active–passive) such as Red Hat Cluster Suite, SIOS, and so on, follow these steps. (In the example, suppose that the Oracle database is running on a Red Hat cluster that has cluster services running on two nodes, with one being active where the database is running and the other being passive.)

Active-passive cluster solutions

To implement active-passive cluster solutions, complete the following steps:

1. Install the plug-in manually on the Oracle host. Confirm that the SnapCenter Server IP and the SPL_ENABLED_PLUGINS have the correct values for the `/var/opt/SnapCenter/spl/etc/spl.properties` file.

```
SNAPCENTER_SERVER_HOST=10.232.206.110
SPL_ENABLED_PLUGINS=SCO,SCU
```

2. Use `sccli` to set the preferred IPs of all the cluster nodes and the host, including the floating IP:

```
Sccli Set-PreferredHostIPsInStorageExportPolicy -IpAddresses
'10.231.73.50','10.231.73.51','10.231.73.52'
```

   – `10.231.73.51` is the floating IP that is being accessed by all the cluster nodes.

   – `10.231.73.52` is the public IP of the second cluster node, which is passive, and `10.231.73.50` is the public IP address of the first node, which is actively hosting the database.

3. Repeat steps 1 and 2 on the second cluster node.
4. Add a local entry of floating IP `10.231.73.51` with some common host name (FQDN)—for example, Linux-cluster.netapp.com— in the host file (`C:\Windows\System32\drivers\etc`) of SnapCenter Server running on Windows. No node entries are required because the SnapCenter operations are completely carried over floating IP or VIP and therefore are not dependent on the host.
5. Use PowerShell or the GUI to perform the Add Linux Host operation and give the host IP as `10.231.73.51` (floating IP). Select the option to skip the preinstallation check and then complete the registration process. It might take some time (about five minutes) to recognize the plug-in.
6. Refresh the Resources screen to discover all of the Oracle databases running on Node1 (where the current floating IP is running with databases; that is, the active node). You can also create policies and resource groups, start protecting them, and perform backups, restore, and clones.

   During host failover, the Oracle database is migrated to an alternative node in the cluster that is using the floating IP or virtual IP. The backups and clones that were taken earlier on Node1 are still reflected in SnapCenter, regardless of the database being migrated to the second node; it doesn’t really matter because all of the workflows are completely communicated using only VIP.

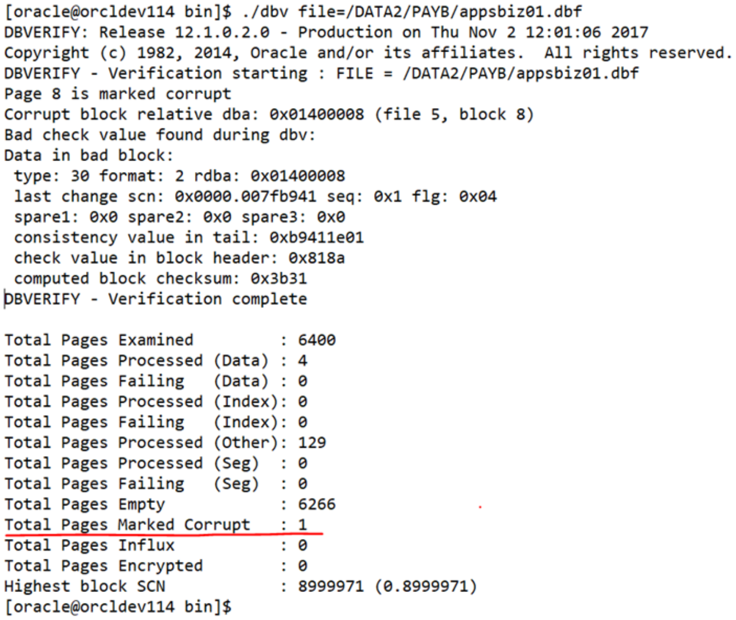
   Similarly, the databases can fall back to Node1 and all backup, restore, mount, and clone functions still work normally.

Appendix C: Advanced recovery (block level, table, and tablespace level point-in time recovery)

Block-level recovery

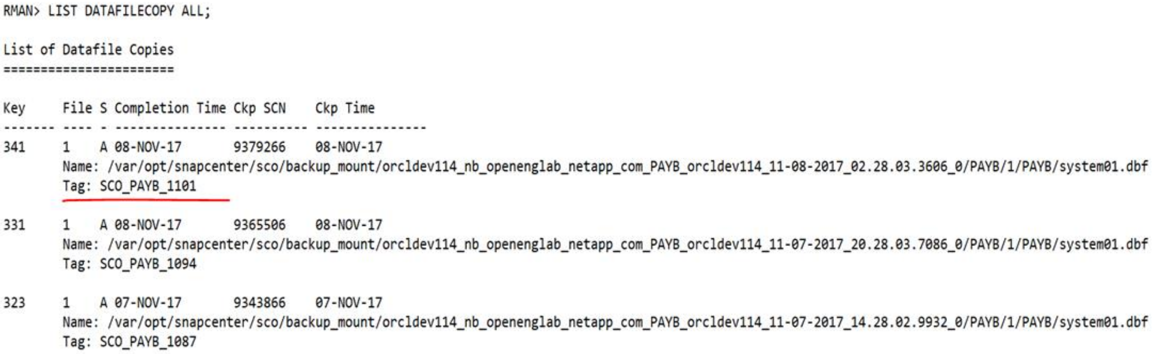
You can perform block-level recovery by using these RMAN cataloged Snapshot copies. The following steps are an example of how to perform block level recovery:

1. Use the `dbv` utility to check the data file that has a corrupt block.



```
[oracle@orcldev114 bin]$ ./dbv file=/DATA2/PAYB/appsbiz01.dbf
DBVERIFY: Release 12.1.0.2.0 - Production on Thu Nov 2 12:01:06 2017
Copyright (c) 1982, 2014, Oracle and/or its affiliates.  All rights reserved.
DBVERIFY - Verification starting : FILE = /DATA2/PAYB/appsbiz01.dbf
Page 8 is marked corrupt
Corrupt block relative dba: 0x01400008 (file 5, block 8)
Bad check value found during dbv:
Data in bad block:
 type: 30 format: 2 rdba: 0x01400008
 last change scn: 0x0000.007fb941 seq: 0x1 flg: 0x04
 spare1: 0x0 spare2: 0x0 spare3: 0x0
 consistency value in tail: 0xb9411e01
 check value in block header: 0x818a
 computed block checksum: 0x3b31
DBVERIFY - Verification complete

Total Pages Examined         : 6400
Total Pages Processed (Data) : 4
Total Pages Failing   (Data) : 0
Total Pages Processed (Index): 0
Total Pages Failing   (Index): 0
Total Pages Processed (Other): 129
Total Pages Processed (Seg)  : 0
Total Pages Failing   (Seg)  : 0
Total Pages Empty            : 6266
Total Pages Marked Corrupt   : 1
Total Pages Influx           : 0
Total Pages Encrypted        : 0
Highest block SCN            : 8999971 (0.8999971)
[oracle@orcldev114 bin]$
```

Note: Use the following commands to list the backups that are taken through SnapCenter and cataloged with RMAN:

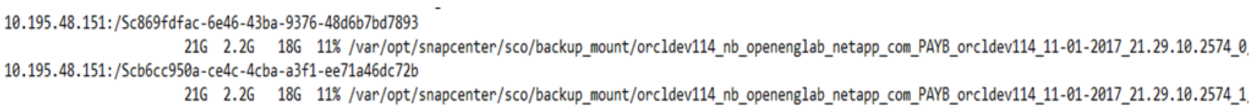


```
RMAN> LIST DATAFILECOPY ALL;

List of Datafile Copies
=======================

Key     File S Completion Time Ckp SCN    Ckp Time
------- ---- - --------------- ---------- ---------------
341     1    A 08-NOV-17       9379266    08-NOV-17
        Name: /var/opt/snapcenter/sco/backup_mount/orcldev114_nb_openenglab_netapp_com_PAYB_orcldev114_11-08-2017_02.28.03.3606_0/PAYB/1/PAYB/system01.dbf
        Tag: SCO_PAYB_1101

331     1    A 08-NOV-17       9365506    08-NOV-17
        Name: /var/opt/snapcenter/sco/backup_mount/orcldev114_nb_openenglab_netapp_com_PAYB_orcldev114_11-07-2017_20.28.03.7086_0/PAYB/1/PAYB/system01.dbf
        Tag: SCO_PAYB_1094

323     1    A 07-NOV-17       9343866    07-NOV-17
        Name: /var/opt/snapcenter/sco/backup_mount/orcldev114_nb_openenglab_netapp_com_PAYB_orcldev114_11-07-2017_14.28.02.9932_0/PAYB/1/PAYB/system01.dbf
        Tag: SCO_PAYB_1087
```

Note: Select a data file copy with an SCO prefixed tag that matches to the earliest recovery point and mount that data backup by using SnapCenter to the Oracle host for block-level restore.

Note: If logs on the active file system are already pruned, you can mount the respective log backups for recovery. For information about how to use SnapCenter to mount the data and log backup, see the section titled, “Archive log management for replaying multiple log backups.”

Note: After the backups are mounted on the host, you can verify by running `df -h`. It should look similar to this example:

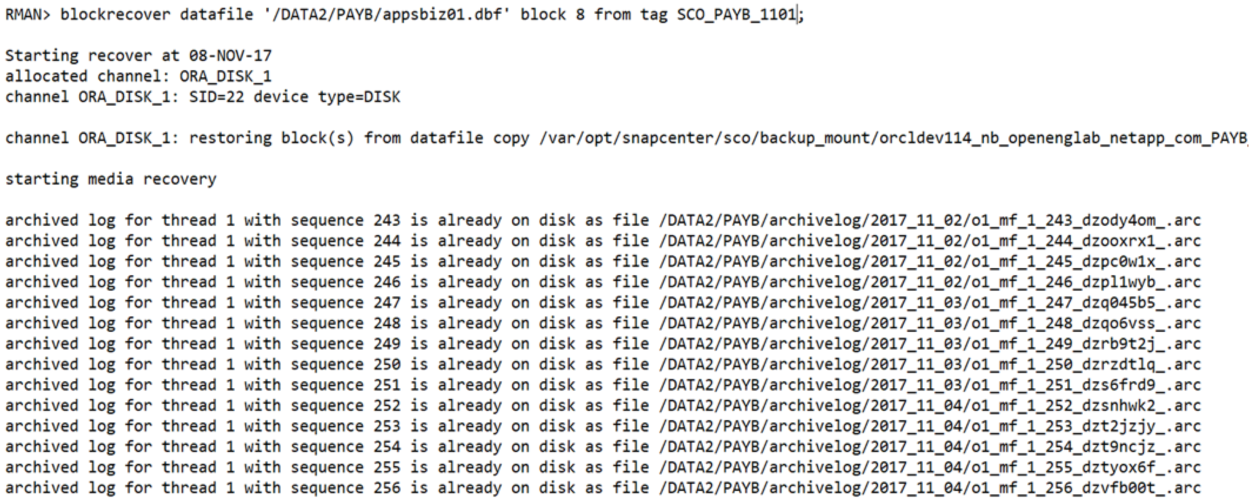


```
10.195.48.151:/Sc869fdfac-6e46-43ba-9376-48d6b7bd7893
                      21G  2.2G   18G  11% /var/opt/snapcenter/sco/backup_mount/orcldev114_nb_openenglab_netapp_com_PAYB_orcldev114_11-01-2017_21.29.10.2574_0
10.195.48.151:/Scb6cc950a-ce4c-4cba-a3f1-ee71a46dc72b
                      21G  2.2G   18G  11% /var/opt/snapcenter/sco/backup_mount/orcldev114_nb_openenglab_netapp_com_PAYB_orcldev114_11-01-2017_21.29.10.2574_1
```

Note: If the logs are not cataloged with RMAN, you have two options:

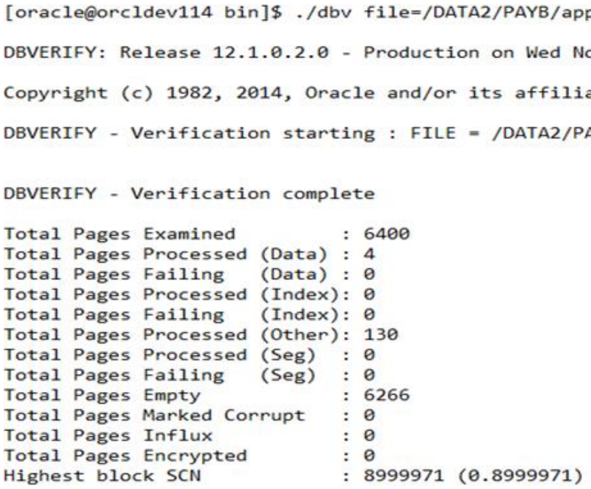
- Copy the archived logs to the required destination and pass the location in the RMAN recovery.
- Manually RMAN catalog the location or files of the mounted archive log destination.

When you have done this, invoke the recovery command:



```
RMAN> blockrecover datafile '/DATA2/PAYB/appsbiz01.dbf' block 8 from tag SCO_PAYB_1101;

Starting recover at 08-NOV-17
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=22 device type=DISK

channel ORA_DISK_1: restoring block(s) from datafile copy /var/opt/snapcenter/sco/backup_mount/orcldev114_nb_openenglab_netapp_com_PAYB

starting media recovery

archived log for thread 1 with sequence 243 is already on disk as file /DATA2/PAYB/archivelog/2017_11_02/o1_mf_1_243_dzody4om_.arc
archived log for thread 1 with sequence 244 is already on disk as file /DATA2/PAYB/archivelog/2017_11_02/o1_mf_1_244_dzooxrx1_.arc
archived log for thread 1 with sequence 245 is already on disk as file /DATA2/PAYB/archivelog/2017_11_02/o1_mf_1_245_dzpc0w1x_.arc
archived log for thread 1 with sequence 246 is already on disk as file /DATA2/PAYB/archivelog/2017_11_02/o1_mf_1_246_dzpl1wyb_.arc
archived log for thread 1 with sequence 247 is already on disk as file /DATA2/PAYB/archivelog/2017_11_03/o1_mf_1_247_dzq045b5_.arc
archived log for thread 1 with sequence 248 is already on disk as file /DATA2/PAYB/archivelog/2017_11_03/o1_mf_1_248_dzqo6vss_.arc
archived log for thread 1 with sequence 249 is already on disk as file /DATA2/PAYB/archivelog/2017_11_03/o1_mf_1_249_dzrb9t2j_.arc
archived log for thread 1 with sequence 250 is already on disk as file /DATA2/PAYB/archivelog/2017_11_03/o1_mf_1_250_dzrzdtlq_.arc
archived log for thread 1 with sequence 251 is already on disk as file /DATA2/PAYB/archivelog/2017_11_03/o1_mf_1_251_dzs6frd9_.arc
archived log for thread 1 with sequence 252 is already on disk as file /DATA2/PAYB/archivelog/2017_11_04/o1_mf_1_252_dzsnhwk2_.arc
archived log for thread 1 with sequence 253 is already on disk as file /DATA2/PAYB/archivelog/2017_11_04/o1_mf_1_253_dzt2jzjy_.arc
archived log for thread 1 with sequence 254 is already on disk as file /DATA2/PAYB/archivelog/2017_11_04/o1_mf_1_254_dzt9ncjz_.arc
archived log for thread 1 with sequence 255 is already on disk as file /DATA2/PAYB/archivelog/2017_11_04/o1_mf_1_255_dztyox6f_.arc
archived log for thread 1 with sequence 256 is already on disk as file /DATA2/PAYB/archivelog/2017_11_04/o1_mf_1_256_dzvfb00t_.arc
```

Note: When the block recovery command is executed, you can use the dbv utility to check for corrupt blocks:



```
[oracle@orcldev114 bin]$ ./dbv file=/DATA2/PAYB/appsbiz01.dbf

DBVERIFY: Release 12.1.0.2.0 - Production on Wed Nov 8 12:53:29 2017

Copyright (c) 1982, 2014, Oracle and/or its affiliates.  All rights reserved.

DBVERIFY - Verification starting : FILE = /DATA2/PAYB/appsbiz01.dbf


DBVERIFY - Verification complete

Total Pages Examined         : 6400
Total Pages Processed (Data) : 4
Total Pages Failing   (Data) : 0
Total Pages Processed (Index): 0
Total Pages Failing   (Index): 0
Total Pages Processed (Other): 130
Total Pages Processed (Seg)  : 0
Total Pages Failing   (Seg)  : 0
Total Pages Empty            : 6266
Total Pages Marked Corrupt   : 0
Total Pages Influx           : 0
Total Pages Encrypted        : 0
Highest block SCN            : 8999971 (0.8999971)
```

Tablespace PiT recovery

The steps for tablespace PiT recovery are similar to those for block-level recovery; the only difference is that you must bring the tablespace offline before running the RMAN recovery command.

1. Use the following RMAN script for tablespace PiT recovery.

```
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/o1_mf_3_7x0wvco6_.log deleted
auxiliary instance file /tmp/TSPITR_HRA_SFFT/onlinelog/o1_mf_2_7x0wvbjq_.log deleted
auxiliary instance file /tmp/TSPITR_HRA_SFFT/onlinelog/o1_mf_1_7x0wv93y_.log deleted
auxiliary instance file /tmp/TSPITR_HRA_SFFT/datafile/o1_mf_temp_7x0wvf9n_.tmp deleted
```

Note: After recovering the tablespace, bring it back online and perform sanity checks. This entire operation is now natively supported in SnapCenter 4.4 release with complete orchestration.

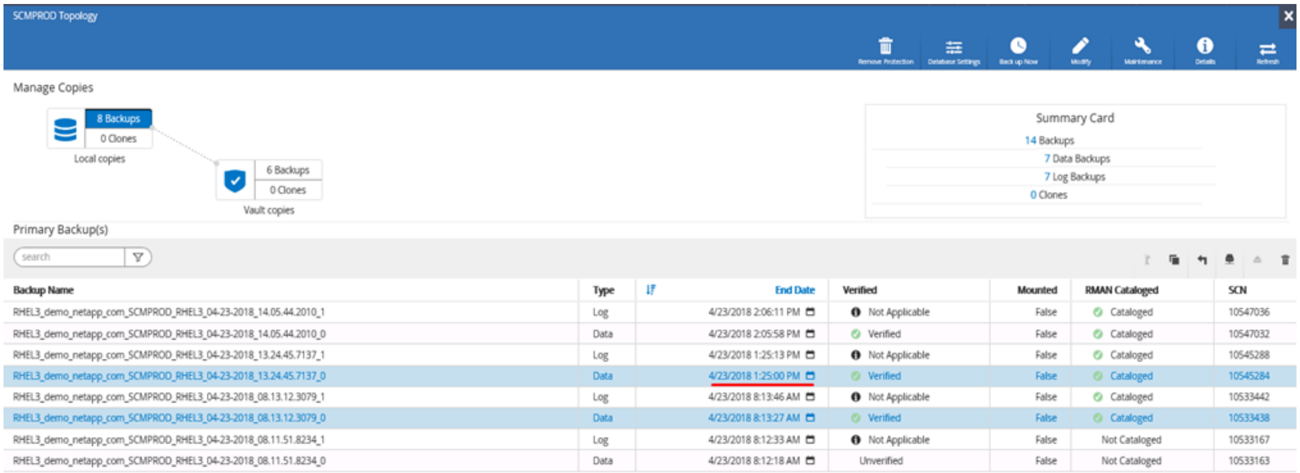
Recover a table

This section describes how to recover a corrupted, deleted, or dropped table.

Recover a corrupted or dropped table by using RMAN cataloged Snapshot copies

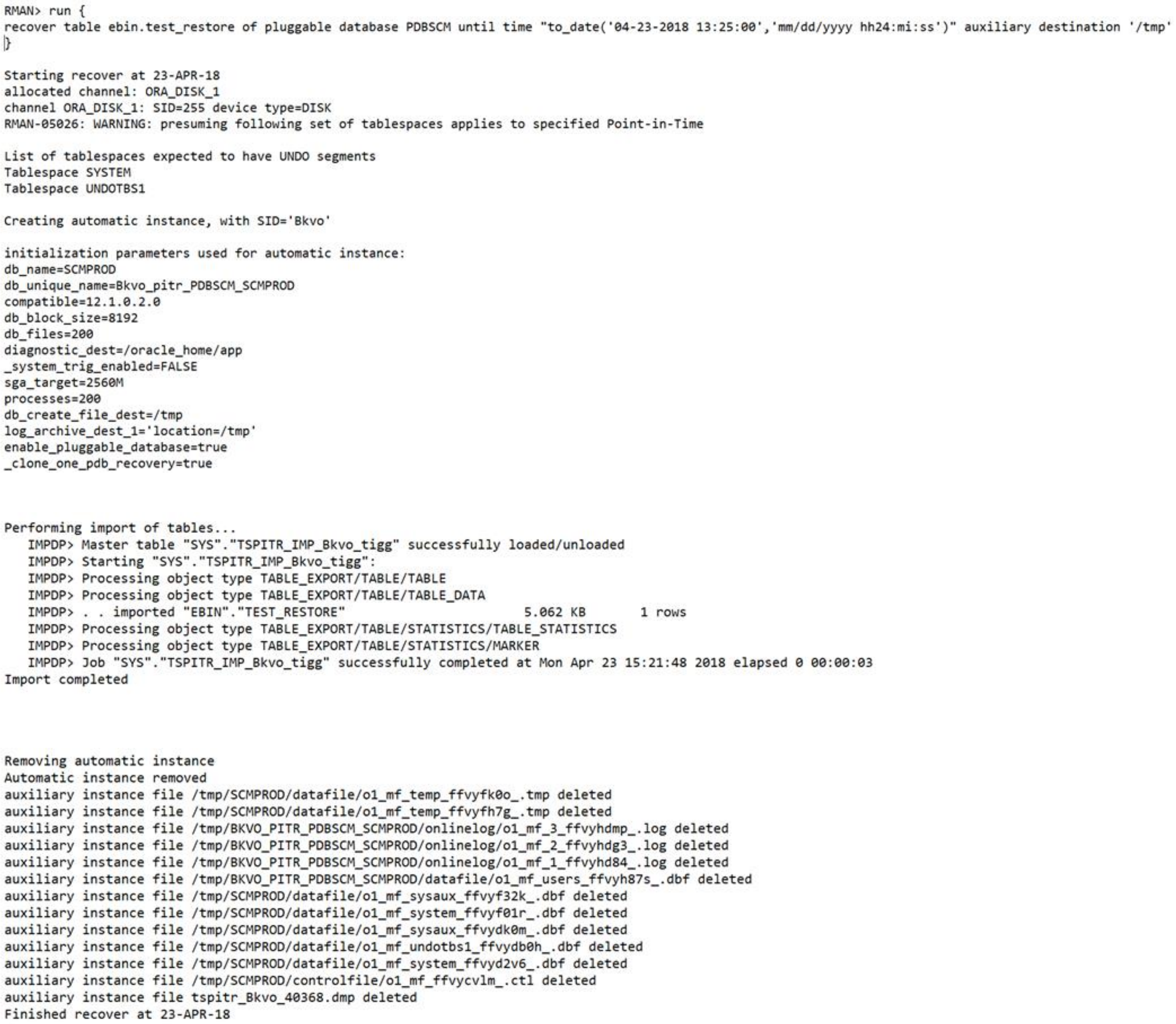
In this scenario, a table is dropped and must be recreated from an existing online backup by using RMAN recovery commands.

1. To restore a table from the backup, use SnapCenter on the Oracle host to mount the data file backup. To perform PiT recovery, the logs must be present in the active file system. If logs are already pruned, mount the log backups to the Oracle host.



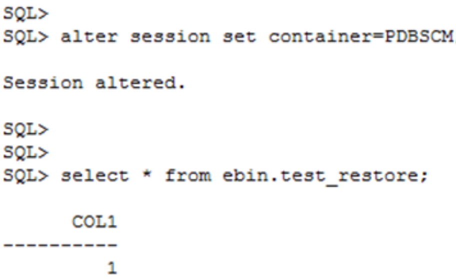
Backup Name	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_14.05.44.2010_1	Log	4/23/2018 2:06:11 PM	Not Applicable	False	✓ Cataloged	10547036
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_14.05.44.2010_0	Data	4/23/2018 2:05:58 PM	✓ Verified	False	✓ Cataloged	10547032
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_13.24.45.7137_1	Log	4/23/2018 1:25:13 PM	Not Applicable	False	✓ Cataloged	10545288
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_13.24.45.7137_0	Data	4/23/2018 1:25:00 PM	✓ Verified	False	✓ Cataloged	10545284
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_08.13.12.3079_1	Log	4/23/2018 8:13:46 AM	Not Applicable	False	✓ Cataloged	10533442
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_08.13.12.3079_0	Data	4/23/2018 8:13:27 AM	✓ Verified	False	✓ Cataloged	10533438
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_08.11.51.8234_1	Log	4/23/2018 8:12:33 AM	Not Applicable	False	Not Cataloged	10533167
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_08.11.51.8234_0	Data	4/23/2018 8:12:18 AM	Unverified	False	Not Cataloged	10533163

Note: Select the data file backup that is closest to your requirement and mount it to the Oracle host, then execute the recovery command:



```
RMAN> run {
recover table ebin.test_restore of pluggable database PDBSCM until time "to_date('04-23-2018 13:25:00','mm/dd/yyyy hh24:mi:ss')" auxiliary destination '/tmp'
}

Starting recover at 23-APR-18
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=255 device type=DISK
RMAN-05026: WARNING: presuming following set of tablespaces applies to specified Point-in-Time

List of tablespaces expected to have UNDO segments
Tablespace SYSTEM
Tablespace UNDOTBS1

Creating automatic instance, with SID='Bkvo'

initialization parameters used for automatic instance:
db_name=SCMPROD
db_unique_name=Bkvo_pitr_PDBSCM_SCMPROD
compatible=12.1.0.2.0
db_block_size=8192
db_files=200
diagnostic_dest=/oracle_home/app
_system_trig_enabled=FALSE
sga_target=2560M
processes=200
db_create_file_dest=/tmp
log_archive_dest_1='location=/tmp'
enable_pluggable_database=true
_clone_one_pdb_recovery=true



Performing import of tables...
   IMPDP> Master table "SYS"."TSPITR_IMP_Bkvo_tigg" successfully loaded/unloaded
   IMPDP> Starting "SYS"."TSPITR_IMP_Bkvo_tigg":
   IMPDP> Processing object type TABLE_EXPORT/TABLE/TABLE
   IMPDP> Processing object type TABLE_EXPORT/TABLE/TABLE_DATA
   IMPDP> . . imported "EBIN"."TEST_RESTORE"                       5.062 KB       1 rows
   IMPDP> Processing object type TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
   IMPDP> Processing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER
   IMPDP> Job "SYS"."TSPITR_IMP_Bkvo_tigg" successfully completed at Mon Apr 23 15:21:48 2018 elapsed 0 00:00:03
Import completed



Removing automatic instance
Automatic instance removed
auxiliary instance file /tmp/SCMPROD/datafile/o1_mf_temp_ffvyfk0o_.tmp deleted
auxiliary instance file /tmp/SCMPROD/datafile/o1_mf_temp_ffvyfh7g_.tmp deleted
auxiliary instance file /tmp/BKVO_PITR_PDBSCM_SCMPROD/onlinelog/o1_mf_3_ffvyhdmp_.log deleted
auxiliary instance file /tmp/BKVO_PITR_PDBSCM_SCMPROD/onlinelog/o1_mf_2_ffvyhdg3_.log deleted
auxiliary instance file /tmp/BKVO_PITR_PDBSCM_SCMPROD/onlinelog/o1_mf_1_ffvyhd84_.log deleted
auxiliary instance file /tmp/BKVO_PITR_PDBSCM_SCMPROD/datafile/o1_mf_users_ffvyh87s_.dbf deleted
auxiliary instance file /tmp/SCMPROD/datafile/o1_mf_sysaux_ffvyf32k_.dbf deleted
auxiliary instance file /tmp/SCMPROD/datafile/o1_mf_system_ffvyf01r_.dbf deleted
auxiliary instance file /tmp/SCMPROD/datafile/o1_mf_sysaux_ffvydk0m_.dbf deleted
auxiliary instance file /tmp/SCMPROD/datafile/o1_mf_undotbs1_ffvydb0h_.dbf deleted
auxiliary instance file /tmp/SCMPROD/datafile/o1_mf_system_ffvyd2v6_.dbf deleted
auxiliary instance file /tmp/SCMPROD/controlfile/o1_mf_ffvycvlm_.ctl deleted
auxiliary instance file tspitr_Bkvo_40368.dmp deleted
Finished recover at 23-APR-18
```

Note: After recovering the table, verify whether the table exists with exact records.



```
SQL>
SQL> alter session set container=PDBSCM;

Session altered.

SQL>
SQL>
SQL> select * from ebin.test_restore;

      COL1
----------
         1
```

Recreate a dropped table by exporting it from a clone of a backup

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

1. Use the GUI or CLI to create a clone of the target Oracle database on the same or a remote host. For more information, see the steps in the section titled, “Oracle database clone and refresh best practices.”

   Note: 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
```

   Note: 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
```

Recreate a dropped table from a clone of a backup by using a database link

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

1. Use the GUI or CLI to create a clone of the target Oracle Database on the same or a remote host. For more information, see the steps in the section titled, “Oracle database clone and refresh best practices.”

   Note: When the clone is complete, manually add an entry for the clone database (for example, `apr12cln`) in the `tnsnames.ora` file.

   Note: Create a database link in the target database to the clone database:

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

   Note: Select from the table in the clone database and use the database link to recreate the dropped table in the target database:

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

Appendix D: Restore from secondary SnapMirror or vault storage

As described in the section titled, “SnapCenter backup policies and resource group best practices,” there are two options to protect backups for near-term retention in secondary storage, in a vault and/or disaster recovery destination. To understand the restore use cases from secondary, it is important to understand why the Snapshot copy must be replicated to secondary storage. Here are the few cases:

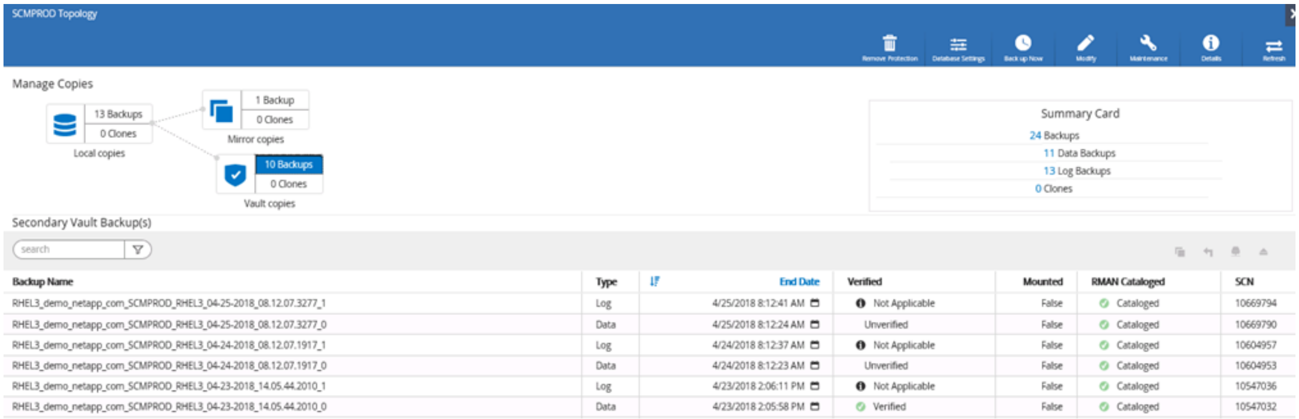
- Snapshot copies in primary storage are useful for quicker recovery time objectives (RTOs). Mission-critical systems with narrow RTOs demand efficient recovery point objectives (RPOs), where backups are taken at very frequent intervals. This situation might easily reach the limit of 1,024 Snapshot copies, so retaining more backups on primary storage might not be possible. In such cases, you should replicate daily or weekly backups to secondary vault and/or disaster recovery storage.
- Replicating to a disaster recovery site (mirror destination)—that is, mirroring all Snapshot copies supported by SnapCenter — is useful to bring up a database in a secondary site in the event of a disaster.

- Vaulting a Snapshot copy helps to achieve a near-tape solution. It is much faster than tape for restores and cloning, but not in storing a number of backups for more than seven years (with optimum method of storing daily, weekly, monthly, and yearly). You can perform clones and restores with similar performance to that of the primary.

  Note: For vault, mirror, and unified replication, you can perform restores and clones from both SnapCenter and storage. If protection is done outside of SnapCenter (you have taken Snapshot copies directly from the primary storage and enabled schedules to replicate them to the secondary destination), it might be necessary to manually perform all the steps for restore or clone from storage; you cannot leverage SnapCenter.

- In SnapCenter, you can choose backups between primary and secondary storage for restores. Here are two reasons to choose backups from the mirror or vault destination for restore and recovery:
  - The availability of storage or storage failure at the production site.
  - The availability of Snapshot copies on the primary storage; that is, if Snapshot copies are already deleted on the primary storage based on the retention settings.

Here is an extract of the topology view representing the backups located at different storage destinations (primary/local, secondary vault, and secondary mirror), with the vault destination selected.



Summary Card
24 Backups
11 Data Backups
13 Log Backups
0 Clones

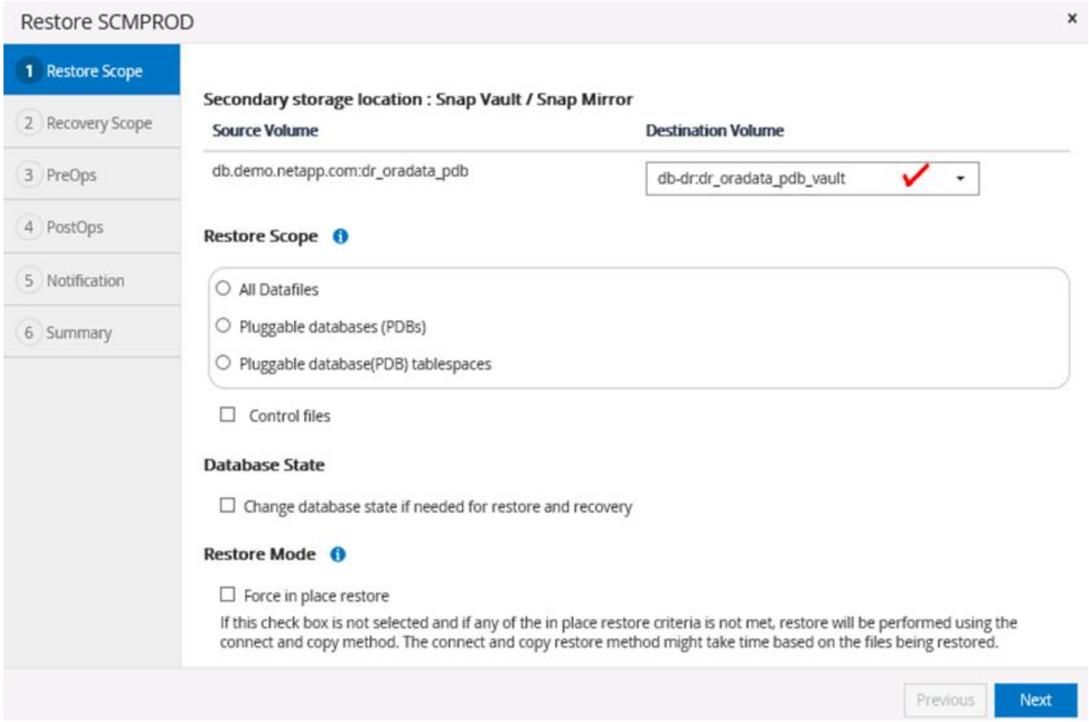
Secondary Vault Backup(s)

Backup Name	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_08.12.07.3277_1	Log	4/25/2018 8:12:41 AM	Not Applicable	False	Cataloged	10669794
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-25-2018_08.12.07.3277_0	Data	4/25/2018 8:12:24 AM	Unverified	False	Cataloged	10669790
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-24-2018_08.12.07.1917_1	Log	4/24/2018 8:12:37 AM	Not Applicable	False	Cataloged	10604957
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-24-2018_08.12.07.1917_0	Data	4/24/2018 8:12:23 AM	Unverified	False	Cataloged	10604953
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_14.05.44.2010_1	Log	4/23/2018 2:06:11 PM	Not Applicable	False	Cataloged	10547036
RHEL3_demo_netapp_com_SCMPROD_RHEL3_04-23-2018_14.05.44.2010_0	Data	4/23/2018 2:05:58 PM	Verified	False	Cataloged	10547032

Restore from a secondary vault destination

To restore from a secondary vault destination, complete the following steps:

1. Select a data backup and click the Restore button.



Restore SCMPROD

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
db.demo.netapp.com:dr_oradata_pdb	db-dr:dr_oradata_pdb_vault ✓

Restore Scope

○ All Datafiles
○ Pluggable databases (PDBs)
○ Pluggable database(PDB) tablespaces

□ Control files

Database State

□ Change database state if needed for restore and recovery

Restore Mode

□ Force in place restore

If this check box is not selected and if any of the in place restore criteria is not met, restore will be performed using the connect and copy method. The connect and copy restore method might take time based on the files being restored.

Note: In the Restore wizard, notice the mapping of the source volume and destination volume in the secondary storage location. Because you selected Snapshot copies from the vault destination, the wizard selected the vault destination volume. Similarly, if the Snapshot copy was selected from the mirror destination, the wizard would show mirror destination volumes. If you have both, you can change the destination volume from vault to mirror.

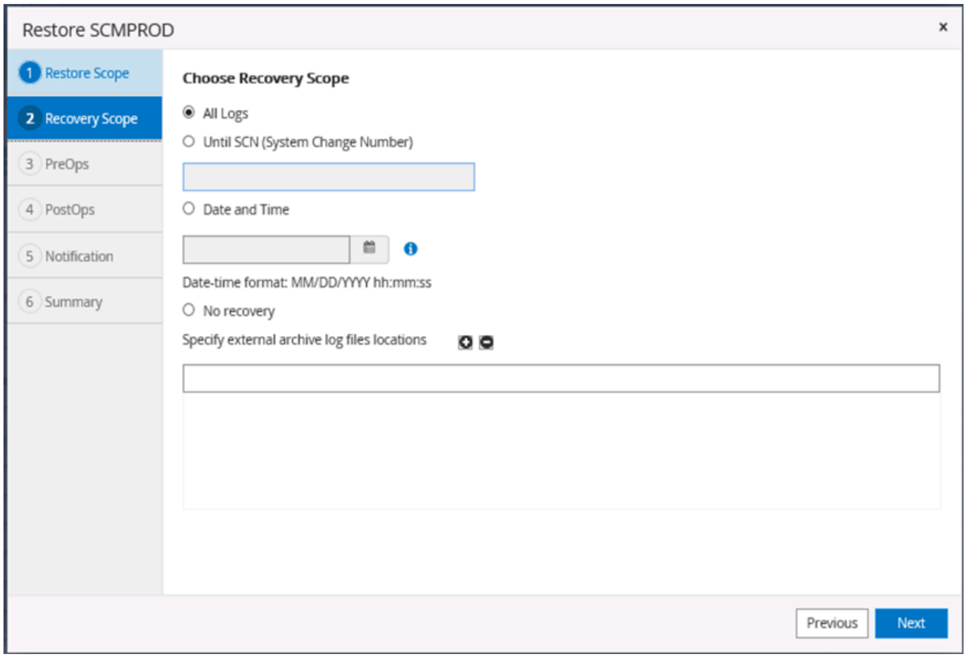
The Restore Scope window contains options: If you selected all data files plus the control file, it’s a full database restore of the legacy or the entire CDB database. If you have selected a multitenant database for restore, you have the option to choose either PDB or PDB tablespace.

a. Use the Change Database State option to bring the database offline during a complete database restore if the database is up and running.

b. Use the Restore Mode option to enforce an in-place restore (faster restore mechanism), even if it can’t meet fast restore requirements due to foreign file constraints. If foreign files like non-Oracle files or backup copies or files from a different Oracle Database exist on the same LUN as the actual database to be restored, the default connect and copy approach to fast restore is overridden, thus removing all files that were newly created and not part of the regular backup. On the contrary, if any of the Oracle files of the actual database exist or share the same volume/LUN, fast restore is not performed despite the checkbox being selected. Therefore the connect and copy approach is used in such cases. For more information about the mechanism and importance of restore-friendly layouts, refer to section 10,Oracle Clone Best Practices.

The Recovery Scope window contains four options:

– **All Logs.** This option applies to all the logs present in the active file system for recovery. If you have passed any external archive log file locations, it applies the logs present in that mounted location and then applies the remaining logs until the latest available in the active file system.



Restore SCMPROD

1 Restore Scope
2 Recovery Scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Choose Recovery Scope

● All Logs

○ Until SCN (System Change Number)

○ Date and Time

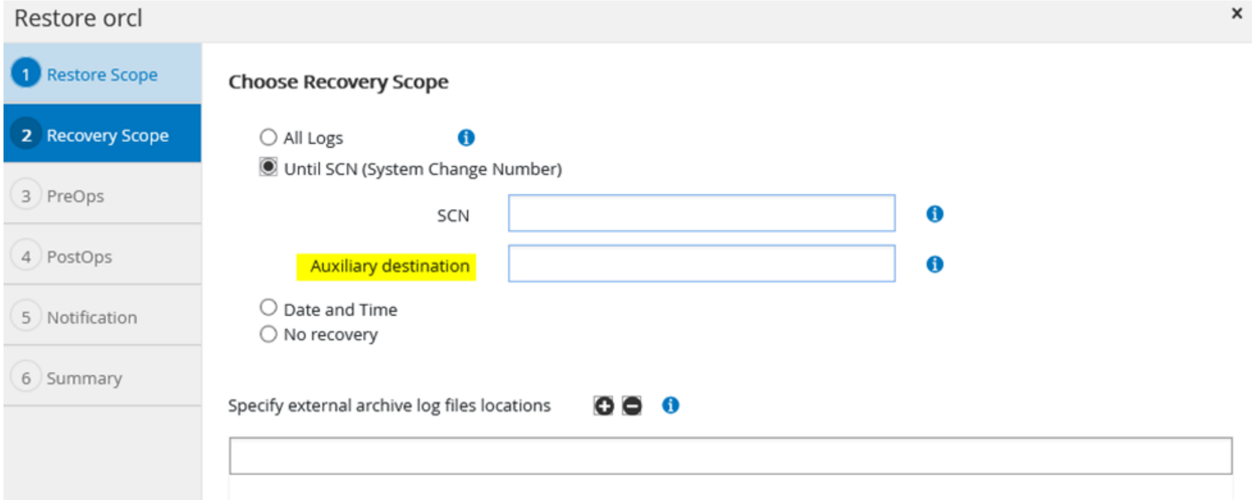
Date-time format: MM/DD/YYYY hh:mm:ss

○ No recovery

Specify external archive log files locations

– **Until SCN.** This option checks through the logs in the active file system or from immediate log backup that is mounted have this SCN. If the required consistency isn’t present in the existing log backup, you must mount other log backups and pass the location in the external log location.

Starting with SnapCenter 4.4, support for PiTR and SCN-based recovery for tablespaces and PDBs are included. To perform thin clone of the database to perform the required object restore, you must additionally provide the auxiliary destination for RMAN.



Restore orcl

1 Restore Scope
2 Recovery Scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Choose Recovery Scope

○ All Logs

● Until SCN (System Change Number)

SCN

Auxiliary destination

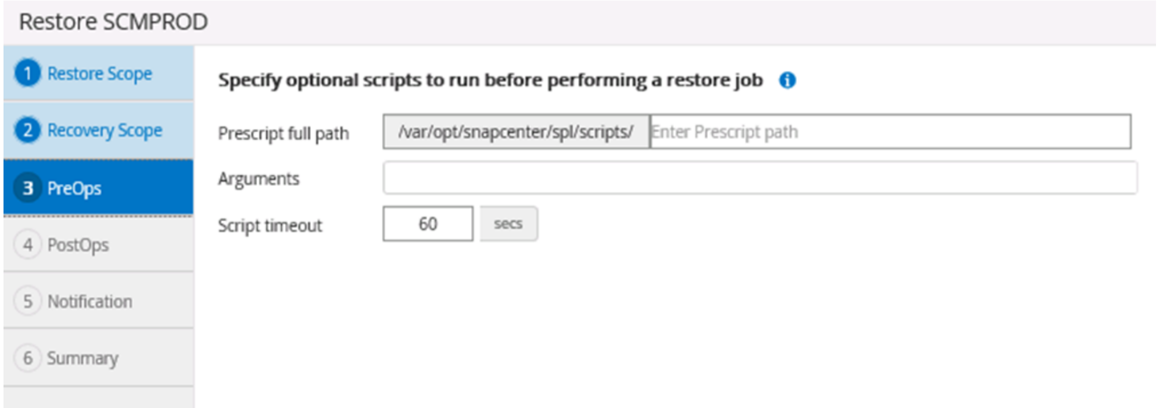
○ Date and Time

○ No recovery

Specify external archive log files locations

– **No recovery.** SnapCenter performs only the restore operation of all data files, tablespace, or PDBs; it doesn’t perform recovery. This option is useful for administrators to perform manual recovery by using Oracle SQLPLUS/RMAN.

(Optional) On the PreOps page, specify any scripts that you want to run before the restore operation.


Restore SCMPROD

Specify optional scripts to run before performing a restore job

Prescript full path: /var/opt/snapcenter/spl/scripts/ Enter Prescript path

Arguments:

Script timeout: 60 secs

(Optional) On the PostOps page, provision any scripts that should be run after the restore and recovery operation:

a. Select the option to open the database or container database in read-write mode; otherwise you must open the database manually.

b. In the Notification window, configure email alerts for successful and failed operations.

c. Click Finish to submit the job.

You can track the progress of the job in the monitor page or activity panel.

Disaster recovery

Although SnapCenter doesn’t support an orchestrated disaster recovery solution, you can use SnapCenter backups to handle disaster recovery manually. This section describes the steps in the manual recovery of a database in the disaster recovery site.

- If storage alone fails on site A, it might be necessary to break the SnapMirror relationship manually for all the volumes of the database (with the latest application-consistent Snapshot); discover those LUNs as ASM disks; mount them back as ASM disk groups on the host; and bring up the database.
- In the event of failure of an entire site like storage, compute, host, or network, you must break the SnapMirror relationship across the storage layer, using the latest application-consistent Snapshot copy, and bring up the storage on the disaster recovery site.

For better RTO, NetApp recommends keeping the disaster recovery Oracle host ready (in passive mode) to host disaster recovery volumes or LUNs directly. That is, keep a similar compute machine or host with Oracle and grid home patched exactly the same as production. Verify that the network layer changes are handled effectively so that production traffic is redirected to the disaster recovery site. In the case of an ASM-managed production database, NetApp recommends keeping the plain ASM instance up and running passively on the disaster recovery site.

For SAN-based deployment, set the `iscsiadm` connection or FC LUNs to be zoned, so that hosts can discover the LUNs from the storage. These devices that are discovered on the host are already considered as ASM disks, because the SnapMirror relationship has been broken with the latest available application-consistent Snapshot. Next, create the ASM disk group and mount them. Run the recovery command (PITR or SCN based) to bring up the database on the disaster recovery site. For recovery, check that all of the archive logs required for recovery from the data Snapshot are available. If they are not, mount the older Snapshot copies to the host/ASM and catalog them with RMAN for automated recovery.

For NFS layouts, you can directly mount the NFS volumes and run the recovery command by replaying the logs.

If the disaster recovery Oracle host is not ready on the disaster recovery site, you must create a new host and have Oracle grid home (if it is ASM or RAC based) extracted from the source TAR backup. It might be necessary to relink the binaries with the new host. Once the Oracle grid home is ready, repeat step2 to bring up the database by mounting the storage devices to the host or ASM, recreate the disk group, mount them to the ASM instance, and recover the database.

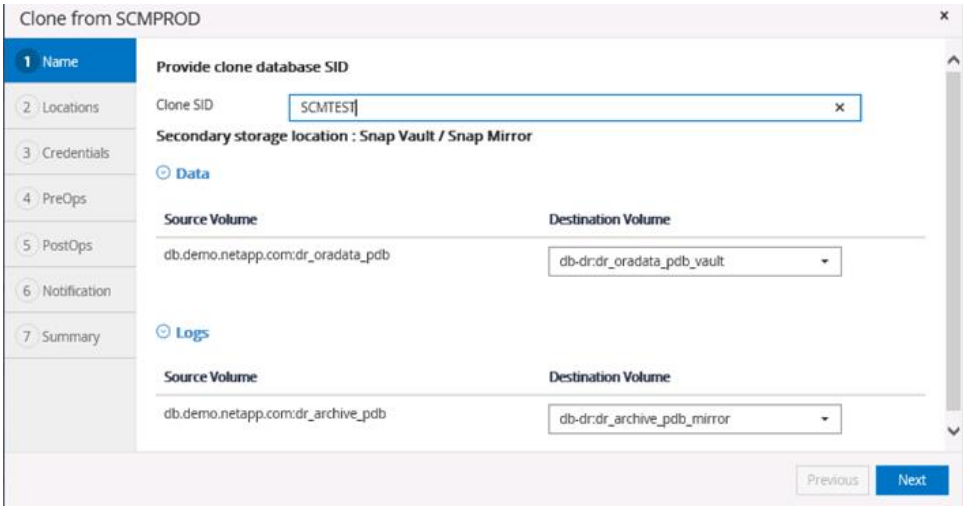
Another alternative is to bring up a clone of the Oracle production database from a secondary disaster recovery or vault-replicated Snapshot. To host a clone to the disaster recovery host, first make sure that the SnapCenter agent for Oracle was installed on that host. Second, Oracle home must have been configured. Third, if the source was an ASM database, the grid home and ASM instance must be up and running on that host. The clone SID can still use the same name as the production database. Once the clone is completed, you can split the clone from the vaulted volumes to get standalone volumes for the database.

Appendix E: Perform a clone operation by using the Clone wizard

To perform a clone operation by using the Clone wizard, complete the following steps:

1. In the Clone wizard, enter the clone SID.

   By default, the Clone wizard populates the storage volume mapping for the source volumes of the given production database. If you have more than one mapping — that is, both SnapMirror and SnapVault — you can still change the destination volume to either vault or mirror volume.



Clone from SCMPROD

Provide clone database SID

Clone SID: SCMTEST

Secondary storage location : Snap Vault / Snap Mirror

Data

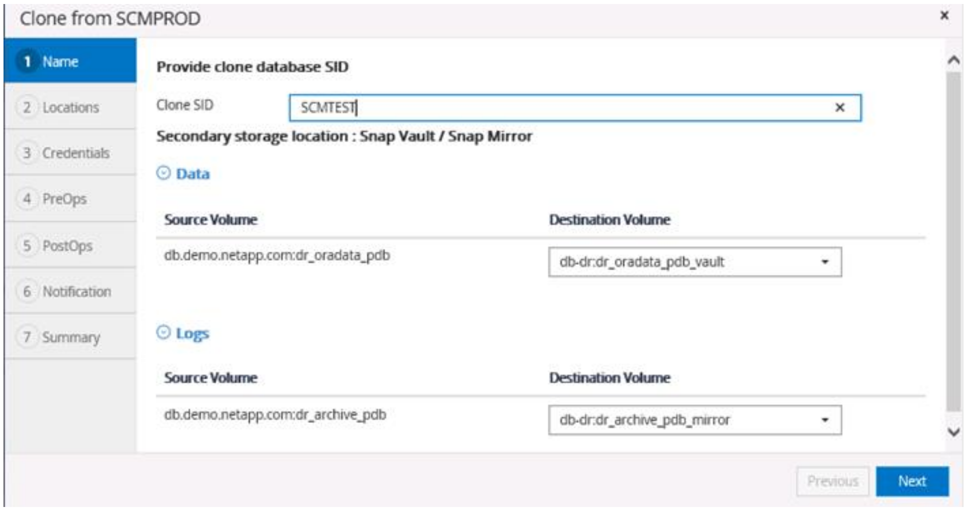
Source Volume	Destination Volume
db.demo.netapp.com:dr_oradata_pdb	db-dr:dr_oradata_pdb_vault

Logs

Source Volume	Destination Volume
db.demo.netapp.com:dr_archive_pdb	db-dr:dr_archive_pdb_mirror

2. On the Locations page, enter the clone host details.

   The clone host can be the same host as that of production, or it can be a different Linux host. If you plan to clone to the same or an alternate host, you must follow the prerequisites. You can customize the directory structure and default values populated for data files, redo log, and control file. If you are cloning in a hybrid cloud environment, the clone Linux host can be in the cloud, such as AWS, Azure, IBM, and so on. The network firewall must be open to listen to the host IPs and the ports. It lives in the primary and secondary storage SVMs that were listed in the preinstallation guidelines in the section titled, “SnapCenter Plug-in for Oracle preinstallation best practices.”



Clone from SCMPROD

Provide clone database SID

Clone SID: SCMTEST

Secondary storage location : Snap Vault / Snap Mirror

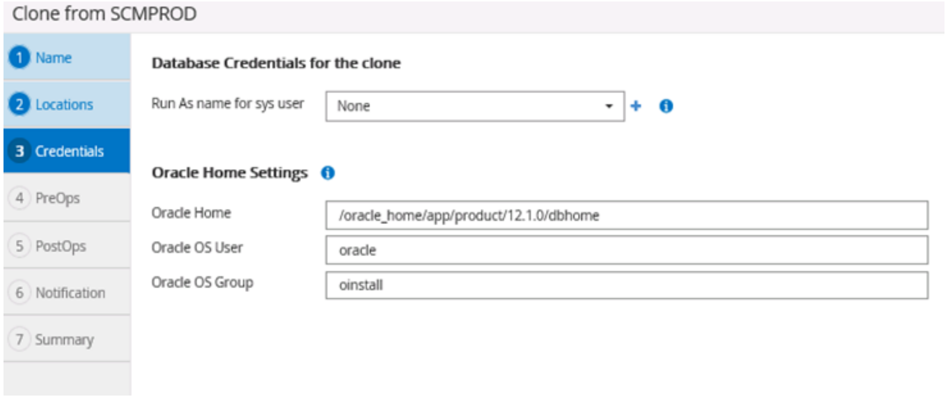
Data

Source Volume	Destination Volume
db.demo.netapp.com:dr_oradata_pdb	db-dr:dr_oradata_pdb_vault

Logs

Source Volume	Destination Volume
db.demo.netapp.com:dr_archive_pdb	db-dr:dr_archive_pdb_mirror

Note: On the Credentials page, enter the details for hosting the clone database: Oracle home, operating system user, and group of the target host. Enter the system credentials for the clone database.



Clone from SCMPROD

Database Credentials for the clone

Run As name for sys user: None

Oracle Home Settings

Oracle Home: /oracle_home/app/product/12.1.0/dbhome

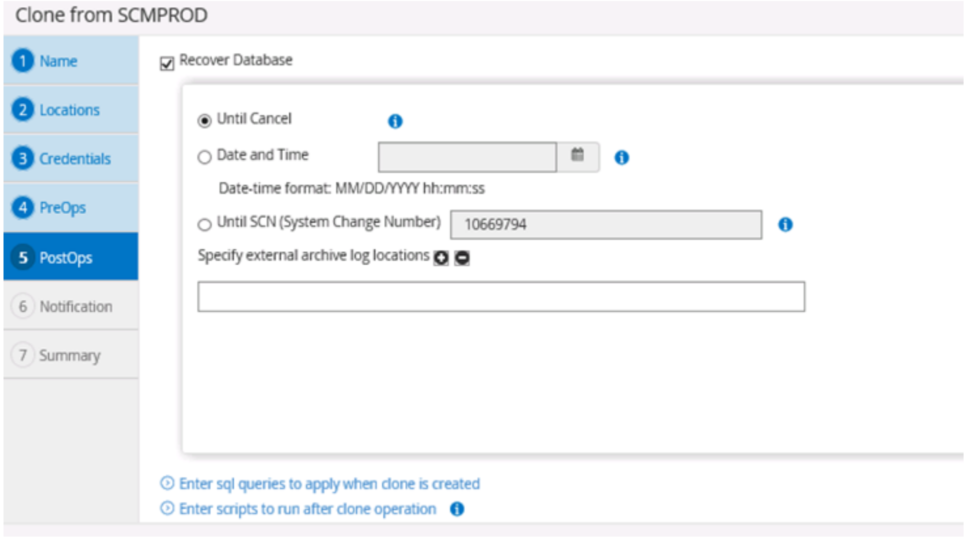
Oracle OS User: oracle

Oracle OS Group: oinstall

Note: (Optional) On the PreOps page, you can provide prescripts that can be run before executing the clone. Any executable scripts, such as Shell, Perl, and Python scripts, are acceptable, but they must be kept in the default location.

Note: (Optional) You can also enter database parameter settings, which are your pfile/spfile settings for the clone database. By default, all the values for each parameter present in the production pfile/spfile are copied. You should add or edit the archive log destination for your clone database, or else the files are placed in the `ORACLE_HOME` destination. Similarly, you should check the SGA, PGA, and open cursors values for the clone database.

Note: (Optional) On the PostOps page, you can opt out of recovery. If you have selected any of the recovery options, SnapCenter automates mounting the immediate archive log backup after the data backup on the target clone host.



Clone from SCMPROD

☑ Recover Database

● Until Cancel

○ Date and Time

Date-time format: MM/DD/YYYY hh:mm:ss

○ Until SCN (System Change Number) 10669794

Specify external archive log locations

Enter sql queries to apply when clone is created

Enter scripts to run after clone operation

- **Until Cancel.** This option applies all the logs in the mounted log backups and brings up the database. By default, it applies logs only from the log backup that was automatically mounted by SnapCenter. For example, to recover to the latest log backups that were taken, mount the log backups manually to the clone host and pass those locations in the external archive log locations.
- **Until Date and Time or SCN.** If you pass date and time or SCN, make sure that the log backup that is mounted by SnapCenter holds good for that recovery point. If it’s part of a different log backup, mount the respective backups on the clone host and pass those locations in external archive log locations.

Note: You can also pass live SQL queries on the PostOps page, along with regular scripts. For example, to delete all HR-sensitive bank or password records, you can write a wrapper shell or Perl script and pass it as postscript for the clone. You can also use the clone wizard or the CLI to automate an end-to-end clone.

Appendix F: RAC-to-RAC clone

A RAC database is cloned as a standalone database by using SnapCenter. It is also possible to convert a non-RAC clone database to a RAC database. It is assumed that the second RAC node is already part of the cluster.

Convert a non-RAC clone database to a RAC database

To convert a non-RAC clone database to a RAC database, complete the following steps:

1. Use the GUI or CLI (non-RAC clone) to perform a regular clone operation.
2. Create redo and undo for the second instance.

```
alter database add logfile thread 2 group 3 ('+DATA’,'+FLASH’) size 50m reuse;
alter database add logfile thread 2 group 4 ('+DATA’,'+FLASH’) size 50m reuse;
alter database enable public thread 2;
create undo tablespace UNDOTBS2 datafile '+DATA' size 50G;
```

a. Add cluster-related parameters in the `init<sid>.ora` file:

```
*.cluster_database_instances=2
*.cluster_database=true
*.remote_listener='LISTENERS_ORCLDB’
ORCLDB1.instance_number=1
ORCLDB2.instance_number=2
```

```
ORCLDB1.thread=1
ORCLDB2.thread=2
ORCLDB1.undo_tablespace='UNDOTBS1'
ORCLDB2.undo_tablespace='UNDOTBS2'
#update the actual controlfile path
*.control_files='+DATA/ORCLDB/controlfile/current.256.666342941','+FLASH/ORCLDB/controlfile/curre
nt.256.662312941'
```

b. Copy the updated `init.ora` file to Node2 and rename the files as per the instance name:

```
[oracle@ora rac1]$ mv initORCLDB.ora initORCLDB1.ora [oracle@orarac2]$ mv initORCLDB.ora
initORCLDB2.ora
```

c. Register the cloned RAC database with `srvctl`:

```
[oracle@orarac1]$ srvctl add database -d ORCLDB -o /u01/app/oracle/product/12.2/db_1
[oracle@orarac1]$ srvctl add instance -d ORCLDB -i ORCLDB1 -n orarac1
[oracle@orarac1]$ srvctl add instance -d ORCLDB -i ORCLDB2 -n orarac2
```

Stop and start the services by using `srvctl` and perform a sanity check by using `crsctl` command.

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

Where to find additional information

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

- Oracle Multitenancy with ONTAP Best practices
- Microsoft documentation about Active Directory Domains and Trusts
https://technet.microsoft.com/en-us/library/cc770299.aspx.
- Oracle Databases on ONTAP TR-3633
https://www.netapp.com/pdf.html?item=/media/8744-tr3633pdf.pdf
- NetApp Interoperability Matrix Tool (IMT)
https://mysupport.netapp.com/matrix/#welcome
- SnapCenter Documentation resources
- SnapCenter Command Reference Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2840882

Version history

Version	Date	Document version history
Version 2.0	February 2021	Revision to previous best practices, new features that include PDB clone/restore, refresh `sm-clone`, and changes to virtualized layout best practices
Version 1.0	June 2018	Initial release.

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

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

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

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

Trademark Information

TR-4700-0221