# Table of Contents

Preface

**Typographical Conventions**

**Introduction** ........................................................................................................... 1

**Overview** .................................................................................................................. 2

**Supported Operations** ............................................................................................... 3
  
  Database Backup (Snap Backup) ................................................................. 3
  Database Restore (Snap Restore) ................................................................. 4
  Database Clone from Snap Backup (Snap Clone) ...................................... 5
  Database Clone from RMAN Backup (RMAN Clone) .............................. 6

**Supported Systems and Configurations** ............................................................. 8

**Supported Storage Systems** ............................................................................... 8

**Special Considerations with Clustered Systems** ............................................. 8

**Supported Oracle Databases** ............................................................................. 9
  
  Supported Database Layouts ........................................................................... 9
  
  Supported Database File Layouts ................................................................. 10
  
  Database Layout and Types of Snap Backups .......................................... 11

**Supported Application (Database) Hosts** ......................................................... 14

**SMU Host Installation Requirements** ................................................................. 15

**Installing the Oracle Snap Management Utility** ............................................... 16

**Installing the Oracle Snap Management Utility on an Oracle Linux Host** ......................................................... 16

**Installing the Oracle Snap Management Utility on Oracle Solaris Hosts** ......................................................... 16

**Installing the Oracle Snap Management Utility on Microsoft Windows Hosts** ......................................................... 17

**Configuring the Snap Management Utility Host and Database Host** ................. 17

**Configuring the Network Port Settings** ............................................................... 18

**Configuring a Windows HTTPS Connection for the Snap Management Utility** ......................................................... 19

**Windows Remote Management Protocol and Service Settings for the Windows Database Host** ......................................................... 19

**Configuring Host System Name Services Recognized by the SMU Host** ............ 21
Enrolling a new application for snap backups .............................................. 39
Modifying an application account ............................................................ 40
Removing an application .......................................................................... 40
Testing an application ............................................................................. 40
Importing an RMAN backup image ............................................................ 40
Deprovisioning an application (clone only) ............................................. 42
Managing Administration Using the BUI ................................................. 43
Adding a new user from the Users tab ..................................................... 43
Modifying a user entry from the Users tab .............................................. 44
Deleting (Remove) a user from the Users tab ......................................... 44
Adding a new notification subscription ..................................................... 45
Modifying a notification subscription from the Notification tab .......... 45
Deleting a notification subscription from the Notifications tab .......... 45
Managing status polling, and task and activity log displays
in the General Settings tab ...................................................................... 46
Operating and Managing Snap Backups in the BUI ................................ 47
Creating a new snap backup ..................................................................... 49
Renaming a snap backup entry .............................................................. 50
Cloning a snap backup entry ................................................................. 50
Rolling back (restoring) a snap backup .................................................... 53
Deleting a snap backup entry ................................................................. 54
Running Simultaneous Snap Operations ............................................... 54
Managing snap backup initiation in the Schedules tab ......................... 54
Adding a schedule .................................................................................... 55
Editing a schedule .................................................................................... 55
Deleting a schedule .................................................................................... 56
Monitoring snap operation tasks .......................................................... 56
Canceling currently running tasks ........................................................ 56
Deleting task history ............................................................................. 56
Managing account settings using the Account Settings tab ................. 56
Managing Activity Logs Using the BUI ................................................. 57
Filtering Activity Logs ............................................................................ 59
Exporting Activity Logs ......................................................................... 60
Purging Activity Logs ............................................................................ 61
Using the Command-Line Interface .................................................. 61
Managing Accounts .............................................................................. 64
Managing Activities .............................................................................. 68
Managing Alerts ..................................................................................... 69
Managing Backups ................................................................................. 71
Managing Certificates ......................................................................... 72
Managing Keys ...................................................................................... 73
Managing Schedules ......................................................................... 74
Managing Tasks .................................................................................... 76
Managing Users ................................................................................... 81
Troubleshooting – General Information ............................................. 83
   SMU Restrictions Quick Reference Table ......................................... 83
Appendix A: References ....................................................................... 87
Appendix B: Glossary ........................................................................... 88
Appendix C: Icon Set for the SMU Browser User Interface .................... 90
Appendix D: Cloning Wallet Files for an Encrypted Database ............ 93
Appendix E: Troubleshooting Common Issues ...................................... 96
Preface

This document is written as a basic guide for database administrators to install, configure and administer Oracle's Snap Management Utility for Oracle Database and presumes a working knowledge of database administration concepts. Further helpful references for the components for which this utility have been designed are included in the References section at the end of this document.

Additionally, for the latest updates and helpful information, users are encouraged to visit the My Oracle Support web site at: http://support.oracle.com.

Typographical Conventions

The following typographical conventions are used throughout this document.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning/Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;italics&gt;</td>
<td>Specifies a variable whose value is supplied by the user. The second example shows less than and greater than signs which are often used to indicate a variable but are not typed.</td>
</tr>
<tr>
<td>monospace</td>
<td>Indicates commands, filenames, directory paths, and executables, and screen code output.</td>
</tr>
<tr>
<td>bold monospace</td>
<td>Indicates a command that the user types.</td>
</tr>
</tbody>
</table>
Introduction

Oracle Snap Management Utility (SMU) for Oracle Database uses the snapshot technology of Oracle ZFS Storage Appliance to allow database administrators (DBAs) to back up, restore, clone, and provision from backup Oracle databases that are hosted on the appliance. Snapshots are read-only virtual copies of a dataset that can be used for two primary purposes: rolling back the dataset to an earlier point in time and creating a new copy of the dataset. In both cases the snapshots and clones share common data blocks with the original dataset. This means that snapshot and clone creation are extremely time and space efficient; creating copies is instantaneous and does not require actually copying any data. Instead, existing data is referenced from the snapshot.

These kinds of on-disk backups created using Oracle Snap Management Utility facilitate quick restore and cloning that is particularly useful for test and development functions. SMU has extended functionality with its ability to provide a database instance from an Oracle Recovery Manager (RMAN) backup resident on an Oracle ZFS Storage Appliance. SMU is not intended to replace Oracle RMAN or other storage backup processes. It is recommended that users supplement the SMU backups with tape or disk backups of the Oracle ZFS Storage Appliance.

SMU is designed for installation and use from the DBA’s management station (terminal or Web browser). This design removes the need for the DBA to coordinate backup, restore and cloning activities with the storage administrator. SMU combines standard host-side processing with storage operations to create seamless functions that simplify the most common administrative tasks the DBA performs. The Snap Management Utility for Oracle Database allows the DBA to directly harness the powerful features of the Oracle ZFS Storage Appliance.
Overview

Oracle Snap Management Utility for Oracle Database leverages Oracle ZFS Storage Appliance technologies to simplify and automate Oracle database backup, recovery, and cloning from backup. SMU benefits the database administrator's task performance with the following features:

- Database and related resource accounts management:
  - Organize and retain account information used to access database resources including the database and storage hosts. SMU operations are tightly integrated so that when the utility executes an operation, it synchronizes its commands among the database, database host, and storage host for zero data loss and consistency.
  - Automatically identify which Oracle ZFS Storage Appliance shares are used by the database, removing the need for the administrator to know the underlying share names.

- Database backup:
  - Create virtually unlimited ZFS snapshot-based backups (limited only by physical system capacity).
  - Schedule backups on a recurring basis.

- Database restore: Reduce the time to restore a database using ZFS rollback.

- Database cloning: Quickly create a database clone for testing or development purposes using ZFS clone.

- Database provisioning from Oracle Recovery Manager (RMAN) backup: Similar to database cloning, but provision a database instance from an RMAN backup.

SMU has the following features:

- Supports both single and Real Application Clusters (RAC) instance databases
- Supports both filesystem (specifically, Network File System [NFS] or direct NFS [dNFS]) and Automatic Storage Management (ASM) (specifically, iSCSI LUN) storage type databases because SMU leverages the unified nature of the Oracle ZFS Storage Appliance
- Creates a variety of types of space-efficient backups and clones using ZFS technology
- Provides the ability to provision new database instances from RMAN backups
Snap Management Utility for Oracle Database provides robust functionality through both command-line interface (CLI) and Browser User Interface (BUI) interfaces. The BUI's navigation tree, operations wizards, menus and icons provide operational details and cues for the existing and required components upon which SMU operates.

Whether using the BUI or CLI, your setup of SMU requires the following basic tasks:

1. Set up accounts. SMU requires a host account for the source Oracle Database instance upon which you may perform operations, and a storage account for the Oracle ZFS Storage Appliance upon which the Oracle Database (host account) resides. Setting up accounts provides the needed permissions as well as configuration to access the database and storage.

2. Enroll applications. Applications are instances of the Oracle databases. Within the accounts, these applications (Oracle databases) are "enrolled" so that the account's administrator can perform tasks on the application (the database instance).

3. Manage administration. Enroll users who may access SMU, and set up their notifications for task events. Also set up monitoring intervals and displays. Likewise, users and notifications can be subsequently deleted or modified, and monitoring settings can be altered.

4. Set up activity logs.

Once these housekeeping activities are accomplished, SMU is set up to perform operations.

Supported Operations

SMU supports the following common database administrative tasks. Each of these tasks uses ZFS technology to eliminate the need to make physical copies of the database blocks, thus saving time and allowing the storage to be used efficiently.

**Important**: Users should not attempt to administer snapshots created by SMU from the Oracle ZFS Storage Appliance. SMU will not use snapshots created from the appliance. SMU will only use the snapshots it has created during its own snap backup operations.

Database Backup (Snap Backup)

SMU can be used to create on-disk backups of databases. The backups are based on ZFS snapshots. This means the backups can be taken quickly and are space efficient. Backups can be created manually or automatically. Automatic backups can be scheduled to occur on a recurring basis. Automatic backups can also employ a retention policy based on the number of backups to retain at a time.

Two types of backups, offline (also referred to as cold backup) and online (also called hot backup) are supported.* Offline backups are backups taken when the database is shut down. The software will shut down
the database temporarily and then restart it after taking the snap backups. Online backups are taken when the
database is placed into backup mode while remaining online.

Online backups take snap backups of the database shares in a particular order and in between changing the
database mode and archiving the current logs. The general steps taken during an online backup are:

1. Place the database into backup mode.
2. Snapshot the datafile shares.
3. Take the database out of backup mode.
4. Archive the current logs.
5. Snapshot the archived log shares.

*Currently, online backups are supported on NFS and dNFS filesystems only.

When creating an offline backup of a clustered database, any database nodes that have been stopped but not
disabled will be restarted at the end of the backup task when SMU restarts the database.

**Database Restore (Snap Restore)**

Using ZFS rollback technology, SMU can restore a database from an on-disk backup, whether it is an offline
snap backup or online snap backup. Rollbacks allow you to revert a dataset back to a point in time without
having to copy or delete any data.

However, because of the way ZFS rollback works, when you perform a restore from a snap backup, any snap
backups that were created after the snap backup you are restoring to are deleted. Additionally, if any of the
snap backups have been cloned, the restore and rename operation cannot be performed and will fail. SMU
will block the rename operation on the snap backup that has clones.

To restore from an offline snap backup, SMU will shut down (abort) the database if it is running, roll back the
shares to the specified snapshot, and then restart the database.

To restore from an online snap backup, SMU will shut down (abort) the database if it is running, roll back the
database shares, start up (mount) the database, create a new controlfile, recover the database, and then open
the database and reset the logs.
Database Clone from Snap Backup (Snap Clone)

SMU can be used to clone a database and create a new primary database. This database is created using ZFS clone technology. ZFS clones are thin-cloned datasets that share common data blocks with the original dataset. This allows the clones to be space efficient and created very quickly.

The clone databases that SMU creates are sized and configured based on the source database. All of the metadata stored with the backup being cloned is used to construct an identical clone of that database.

The following process is used to create a snap clone:

1. Snap backups (share snapshots) are cloned.
2. Clone shares are mounted (if filesystems) or mapped as SCSI disks (if LUNs) on the target database host(s).
3. SMU creates a parameter file for the clone database using input from the user and source parameters stored with the snap backup.
4. SMU starts the clone database.
5. SMU creates a new controlfile for the clone database.
6. SMU recovers the database if necessary.
7. SMU opens the database and resets the logs.
8. SMU recompiles the schema objects. This step allows for creating clones in an environment with a different operating system type from the source database, as long as the supported systems are of the same endian* architecture. (*See Glossary for further information.)
9. SMU adds new temp files.
10. SMU adds or removes undo tablespaces depending on the number of nodes the clone database is using.

Clone filesystem shares are placed in the same project as the source filesystem shares, and clone LUNs are placed in the same initiator and target groups as the source database shares.

When creating a clone database that uses filesystem storage type, SMU will mount the clone shares on the target database host/nodes after they are created on the Oracle ZFS Storage Appliance. In order to mount the shares, SMU must decide which network address to use based on what network interfaces and addresses are configured on the Oracle ZFS Storage Appliance. SMU uses the following algorithm to determine which network address should be used to mount the shares:

1. Look for non-administrative Oracle ZFS Storage Appliance network addresses that are on the same subnet as the database host.
2. Look for non-administrative storage appliance network addresses that are reachable.

3. Look for any storage appliance network address that is on the same subnet as the database host.

4. Look for any storage appliance network address that is reachable.

When cloning a snap backup of an ASM (over iSCSI LUNs) database to a new host, initiators of the new host must be configured in the appropriate iSCSI initiator group and the new host must be already logged in to the appropriate iSCSI target group. When the clone LUNs are created, they are mapped in the same iSCSI initiator and target groups as the original iSCSI LUNs. After the clone LUNs are created, SMU makes the target host scan its SCSI bus to discover the clone LUNs. The clone LUNs will only be visible when the host is logged in to the iSCSI target group.

Linux-based hosts must have the `sg3_utils` package installed. SMU will use the `scsi-rescan` command contained in this package to add and remove clone disks.

Before creating a clone that is dNFS file type, the target Oracle home must first be configured for that type.

SMU provides several options when creating a snap clone:

- Create a database clone on the same host as the original or source database.

- Create the clone on another host (as long as it has the same architecture and Oracle Database software as the source database host). The target host(s) must be using the same type of operating system (endian order; for example, Oracle Linux x86 and Oracle Solaris x86), clusterware (cloud/grid control) version and database software and patch levels as the source database node(s).

- Create a clone that is single instance or clustered. Note that creating a clustered database clone requires that the target host be a node in an existing RAC configuration. Currently, cloning to a RAC One Node configuration is not supported. SMU will perform the necessary conversion steps on the backup used for cloning to make it suitable for a single instance or RAC environment.

**Important**: Only deprovision (delete) a clone database that was created using the SMU from the SMU. Do not delete the database outside of SMU using DBCA (Database Configuration Assistant, a database software tool), for example. SMU needs to connect to and query the clone database before it is deprovisioned.

**Important**: For security reasons, the newly created clone does not automatically inherit the sysdba account from the source database. Only the sys and system users will have automatic access to the new clone.

**Database Clone from RMAN Backup (RMAN Clone)**

SMU can be used to create a new primary database from an RMAN backup for development or testing purposes. The Oracle ZFS Backup Appliance, a hardware variation of the Oracle ZFS Storage Appliance, can be used as a database backup device, especially within Oracle Exadata environments. Database backups on the
Oracle ZFS Storage Appliance or Oracle ZFS Backup Appliance, when they are in image copy format, can be the basis for creating database clones by using ZFS snapshot and clone technology.

You can only create filesystem storage type clone databases using this cloning method.

Requirements for the RMAN backup include:

- The RMAN backup must be in image copy format.
- Backup filenames must be in the %U format specification.
- Backup files must include datafiles, archived log, and controlfile.
- The selected share(s) must contain a single RMAN backup set to be used in the clone operation. No other RMAN files or Oracle files may reside on the share(s).
- The target host(s) for the clone operation must not be the source database node(s).
- The target host(s) must have datapath connectivity to the Oracle ZFS Storage/Backup Appliance.
- The target host(s) must be using the same type of operating system (endian order; for example, Oracle Linux x86 and Oracle Solaris x86), clusterware (cloud/grid control) version and database software and patch levels as the source database node(s).

Note: For detailed information on cross-platform database cloning, see the Oracle Database Backup and Recovery User's Guide 11g Release 1, section 27: "Transporting Data Across Platforms." Refer to the References section at the end of this guide.

RMAN cloning works in the following way:

1. Backup shares are snapped and cloned.
2. Clone shares are mounted on the target host.
3. SMU scans the backup shares to identify the various database files.
4. SMU starts up a temporary database instance so that it can mount the backed-up controlfile. Note that this requires that no database with the same name as the backed-up database already exist on the target host.
5. SMU performs a set of queries against the backup controlfile to get information about the backup. This includes calculating the point to recover the database to (max SCN) and the size the flash recovery area (FRA) should be.
6. After gathering information about the backup, SMU shuts down the temporary instance.
7. SMU creates a parameter file for the clone database.
8. SMU starts the clone database.
9. SMU creates a new controlfile for the clone database.

10. SMU recovers the database.

11. SMU opens the database and resets the logs.

12. SMU re-compiles the schema objects. This step allows for creating clones in an environment with a different operating system type from the source database, as long as the supported systems are of the same endian architecture.

**Important:** Only deprovision (delete) the database clone (from RMAN backup) that was created using the SMU from the SMU. Do *not* delete the database clone outside of SMU using DBCA (Database Configuration Assistant, a database software tool), for example. SMU needs to connect to and query the clone database before it is deprovisioned.

### Supported Systems and Configurations

While Snap Management Utility supports some common administrative tasks performed on Oracle databases utilizing Oracle ZFS Storage appliances, there are important restrictions that must be followed on these systems. Carefully review the following supported systems, configurations, and database file types.

#### Supported Storage Systems

Snap Management Utility supports all models of the Oracle ZFS Storage Appliance, which includes single and clustered systems. SMU does not support third-party storage systems.

The Oracle ZFS Storage Appliance must be running Oracle ZFS Storage Appliance firmware version 2011.1.5 or later.

#### Special Considerations with Clustered Systems

SMU was originally designed to access only one head of a clustered Oracle ZFS Storage Appliance during operations. SMU accesses the head specified in the storage account that is set up in the SMU, and the appropriate pools and shares must be available from that head.

With the version 1.2 release, SMU can administer databases stored on a clustered Oracle ZFS Storage Appliance and which span both heads in an active-active configuration. This feature better supports best practices for achieving high-performance backup operations with systems such as Oracle Exadata.
**Important:** Oracle ZFS Storage clustered appliances must not lock the management interface used by SMU to one head of the cluster; in case of a takeover/failback, the management port must migrate to the active head.

**Supported Oracle Databases**

The Oracle Snap Management Utility supports the following application software:

- Oracle Database 10g R2
- Oracle Database 11g R2

Please note that these following supported versions are minimum versions, and users should always update to the latest releases and patches beyond the minimum supported versions.

Note the following edition support:

- Standard Edition One
- Standard Edition
- Enterprise Edition

_Not supported:_

- Express Edition

Refer to Table 2, Supported Database Configurations, for further Oracle Database version information. This Oracle Database application software must be installed and configured separately.

Snap Management Utility supports both single instance and Oracle Real Application Cluster (Oracle RAC) database configuration types. Oracle RAC One Node database is supported as well.

In Oracle RAC configurations, SMU runs on all nodes in the RAC configurations; users cannot limit/restrict which RAC node SMU runs on.

Note: Common Internet File System (CIFS), used primarily in Microsoft Windows network environments, is not supported by Oracle Database. For more information, refer to [http://docs.oracle.com/cd/E11882_01/win.112/e10845/architec.htm](http://docs.oracle.com/cd/E11882_01/win.112/e10845/architec.htm).

**Supported Database Layouts**

The types of backups that can be performed on a database depend on the database layout. SMU makes no restrictions on the number of shares a database can use. The shares can span projects, pools, and, in the case of clustered storage systems, heads or controllers. There are, however, some restrictions on how files can be...
laid out within those shares. SMU requires that the datafiles and archived logs be in separate shares in order to take online, or hot, backups.

During an online backup, snapshots are taken of the datafile shares first, then a log switch is performed, and then snapshots are taken of the archived logs shares. Because snap backups occur at the share level, the database files must be in different shares in order for this sequencing to work. There are no file restrictions with offline (cold) backups.

Database layout is also an important consideration with database clones created by importing RMAN backups. Clone databases created by importing an RMAN backup will have the same layout as the backup shares: the clone database datafiles will be in clones of the backed-up datafiles’ shares and the clone database archived logs will be in the clones of the backed-up archived log shares. If only a single backup share is used, the datafiles and archived logs will be in the same share.

Consequently, the clone database operation will not support online backups because the files are in the same share. In order to create a clone database that can have online backups taken, there must be at a minimum two backups shares with the backed-up datafiles in one share and the backed-up archived logs in the other share.

Refer to table 1 for the database layouts supported by SMU. SMU requires that each database instance be in separate Oracle ZFS Storage Appliance shares, whether they are NFS/dNFS filesystem or iSCSI LUN shares, and each archiving area must be on separate shares or LUNs from the database. So each application requires two shares, one for the archive and one for the database, and nothing else can reside on those Oracle ZFS Storage Appliance shares.

When SMU performs operations on an Oracle Database, it uses Oracle ZFS Storage Appliance snapshot or clone operations; this is why each database must exist on its own separate set of Oracle ZFS Storage Appliance shares/LUNs. On clone operations SMU mounts the cloned Oracle ZFS Storage Appliance share/LUN on the targeted host and then logs into this server to manipulate the cloned database files to complete the clone operation.

**Supported Database File Layouts**

As detailed in Table 1, SMU requires that these database files be contained in one or more appliance shares:

- datafiles
- controlfiles
- online redo logs
- archived redo logs
Additionally, the datafiles and archived redo log files must be in separate shares in order to support the taking of online snap backups for NFS/dNFS shares. During an online backup, snapshots of the datafile shares are taken first and the archived redo log shares are taken next, along with any other database shares.

Each database must use its own separate set of shares. No two databases can use the same set of shares. SMU performs operations at the appliance share-level using ZFS operations. SMU will not copy, modify or remove individual files in a share. It will only use ZFS operations to clone or snapshot a share. Database oratab file entries

SMU requires that there be an entry in the oratab file for each database it will administer. SMU uses the information in the oratab file to determine the Oracle home of the database. During each SMU operation, SMU will first look up the Oracle home for the database to be operated on by searching the oratab file on the database host. If no entry is found, then the operation will end in an error.

During a cloning operation, SMU will add an entry for the clone database to the local oratab file. The oratab file is located in different locations based on the host operating system:

Oracle Solaris – /var/opt/oracle/oratab
Oracle Linux – /etc/oratab
Microsoft Windows – N/A (Oracle home information is stored in the Windows registry)

Database Layout and Types of Snap Backups

Generally, database backups can be performed when a database is either offline or online. When a database is offline it cannot be updated by users, so there is no potential for new data loss. However, with online (hot) backups, data may be concurrently accessed by users, so a successful backup scenario must accommodate new or changing data capture.

Oracle classifies backups as either consistent or inconsistent. In consistent backups, all files contain the same set of changes. Conversely, inconsistent backups do not contain the same set of changes. Consistent backups are accomplished by shutting down the database and making the backup while the database is closed. This corresponds to an offline or cold backup. Consistent backups do not require recovery when they are used later. Consistent backups are the only valid backup option for databases operating in the NOARCHIVELOG mode.

Inconsistent backups correspond to online or hot backups. These types of backups require recovery – which is the process of making the files consistent – for later use.

For the Snap Management Utility, additional restrictions exist with the database file layouts, depending on which type of snap backups you want to create. The following table describes these restrictions for both
offline (cold) and online (hot) backups. Also refer to the subsection “Database Backup (Snap Backup)” in the section “Supported Operations” for more information.

### TABLE 1. SUPPORTED DATABASE LAYOUTS

<table>
<thead>
<tr>
<th>DATABASE STORAGE TYPE</th>
<th>OFFLINE (COLD) BACKUP</th>
<th>ONLINE (HOT) BACKUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filesystem (NFS/dNFS)</td>
<td>- Database files can be in one or more shares.</td>
<td>- Database datafiles must be in separate shares from the database archived logs.</td>
</tr>
<tr>
<td></td>
<td>- Database files may span shares and pools within the same storage head.</td>
<td>- Database files may span shares and pools within the same storage head.</td>
</tr>
<tr>
<td>ASM</td>
<td>- Database files are in a diskgroup that uses external redundancy and consists of one or more iSCSI LUNs. LUNs must not be partitioned. Cloning with ASM requires Oracle Database version 11.2.0.2 or later.</td>
<td>Not supported.</td>
</tr>
<tr>
<td>FOR BOTH ASM and NFS/dNFS</td>
<td>- Control files, datafiles, and logs (online and archive) must reside on the Oracle ZFS Storage Appliance.</td>
<td></td>
</tr>
</tbody>
</table>

**Important:** Previously, all the shares and LUNs had to reside on only one head of a clustered Oracle ZFS Storage system. With the Snap Management Utility 1.2 release, this is no longer a requirement. Shares can span multiple NAS heads.
The following table shows the supported configurations by host operating system.

**TABLE 2. SUPPORTED DATABASE CONFIGURATIONS BY STORAGE TYPE AND HOST OS**

<table>
<thead>
<tr>
<th>STORAGE TYPE</th>
<th>ORACLE LINUX/RED HAT LINUX (5.5, 5.6, 5.7, 6.3, 6.4)</th>
<th>ORACLE SOLARIS (SOLARIS 10 UPDATE 7 OR LATER)</th>
<th>MICROSOFT WINDOWS (WINDOWS 2008 R2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filesystem (Kernel NFS)</td>
<td>Supported</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Filesystem (Direct NFS)</td>
<td>Requires Oracle Database 11g R2 or later For clone operation in this OS, SMU will not create or modify the oranfstab file, but will only update the system mount table with entries for the clone shares.</td>
<td>Requires Oracle Database 11g R2 or later For clone operation in this OS, SMU will not create or modify the oranfstab file, but will only update the system mount table with entries for the clone shares.</td>
<td>Requires Oracle Database 11g R2 or later; static location layout due to bug 13571798. See My Oracle Support (MOS) at <a href="http://support.oracle.com">http://support.oracle.com</a>, metalink doc 1452760.1 for more information. This release only supports adding single network paths to the filesystem shares in the oranfstab file.</td>
</tr>
</tbody>
</table>
### TABLE 2. SUPPORTED DATABASE CONFIGURATIONS BY STORAGE TYPE AND HOST OS

<table>
<thead>
<tr>
<th>STORAGE TYPE</th>
<th>ORACLE LINUX/RED HAT LINUX (5.5, 5.6, 5.7, 6.3, 6.4)</th>
<th>ORACLE SOLARIS (SOLARIS 10 UPDATE 7 OR LATER)</th>
<th>MICROSOFT WINDOWS (WINDOWS 2008 R2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASM</td>
<td>ASM cloning is not supported on Linux version 5.5. External redundancy only; cloning requires Oracle Database 11.2.0.2 or later due to bug 9316059. Diskgroup members must be physical or raw disks. Virtual Pseudo disks which are used with advanced I/O such as ASMlib, MPIO, logical volume groups, device-mapper, are not supported.</td>
<td>External redundancy only; cloning requires Oracle Database 11.2.0.2 or later due to bug 9316059. Diskgroup members must be physical or raw disks. Virtual Pseudo disks which are used with advanced I/O such as ASMlib, MPIO, logical volume groups, device-mapper, are not supported.</td>
<td>External redundancy only; cloning requires Oracle Database 11.2.0.2 or later due to bug 9316059. Diskgroup members must be physical or raw disks. Virtual Pseudo disks which are used with advanced I/O such as ASMlib, MPIO, logical volume groups, device-mapper, are not supported.</td>
</tr>
</tbody>
</table>

**Note:**

- **ASM_DISKSTRING** parameter settings.
  
  (Use of ASMlib is not supported.)

Parameter default is /dev/rdsk/*. Leave as is.

See My Oracle Support (MOS) at [http://support.oracle.com](http://support.oracle.com) metalink doc 9316059.8 for more information on this bug and other SMU issues.

---

**Supported Application (Database) Hosts**

The Oracle Snap Management Utility supports the following application hosts:

- Oracle Linux/Red Hat Linux (5.5, 5.6, 5.7, 5.8, 6.3, 6.4)
• Oracle Solaris (Solaris 10 Update 7 or later)
• Microsoft Windows (Windows Server 2008 R2)

One of the following must be installed and configured on each application host:

• Windows Remote Shell 2.0 (for Microsoft Windows only)
• Secure Shell 2.x (SSH2) (for Oracle Solaris or Oracle Linux only)

These components are used by the utility to perform remote command execution on the host. They are usually a part of the core operating system and are installed by default. However, if they are not present on the host, you may have to install these components manually.

Oracle Linux and Oracle Solaris hosts do not require any additional configuration.

Microsoft Windows hosts may require additional configuration of the Windows Remote Management Service. The Windows Remote Management (WinRM) Service is started automatically on Windows Server 2008 hosts; however, no WinRM listener is configured by default. A listener must be configured to enable remote management of the host. SMU supports encrypted (HTTPS) listeners only. To enable a listener, follow the steps outlined later in this document under “Configuring a Windows HTTPS Connection.”


In addition to enabling a listener, Windows Remote Management protocol and service settings must be modified for correct SMU operation. These configurations are detailed in the section “Configuring Host Systems to Use the Snap Management Utility” for detailed Microsoft Windows host settings.

SMU Host Installation Requirements

The host system (either application host or management host) on which you install the Snap Management Utility will require the following:

• Oracle Solaris: Solaris 10 (SPARC and x86 editions)
• Linux: Oracle Linux 5 or later
• Microsoft Windows: Windows Server 2008 R2
• 4 GB RAM minimum; 8 GB RAM recommended
• 100 MB free disk space minimum
Java Runtime Environment (JRE) 6 or later

As just noted, the Oracle Snap Management Utility requires JRE 6 or later. You can use the Sun Java Development Kit (JDK), the Sun JRE, or the OpenJDK version of the runtime environment.

Installing the Oracle Snap Management Utility

The Oracle Snap Management Utility is distributed as a set of packages, one package for each supported host environment. The packages are installed using the standard package install command for each environment. You can install the package on the application host or on a separate management host.

Before installing the utility, you must download and extract the software distribution onto the target host or a network location accessible from the target host.

Installing the Oracle Snap Management Utility on an Oracle Linux Host

To install the Oracle Snap Management Utility on a Linux host, perform the following steps.

1. Log in as root (or other privileged user).
   
   $ su
   
   Password:
   
   #

2. Change directory to where the Linux package is located. The same package is used on either 32-bit or 64-bit Linux hosts.
   
   # cd <extract-dir>/Linux/noarch

3. Install the package. In the following command, n.n-nn represents the latest version number of the utility.
   
   # rpm -i oracle-smu-n.n-nn.noarch.rpm

By default, the utility is installed under /opt/oracle/smu.

Installing the Oracle Snap Management Utility on Oracle Solaris Hosts

To install the Oracle Snap Management Utility on Oracle Solaris hosts, perform the following steps:

1. Become root (or other privileged user).
$ su
    Password:
    #

2. Change directory to where the Oracle Solaris package is located.

    # cd <extract-dir>/SunOS/all

3. Install the Oracle Solaris package.

    # pkgadd -d ORCLsmu-n.n-nn.all.pkg all

By default, the utility is installed under /opt/ORCLsmu.

Installing the Oracle Snap Management Utility on Microsoft Windows Hosts

To install the Oracle Snap Management Utility on Windows hosts, perform the following steps:

1. Change to the folder where the Windows package is located.

2. Double click the setup program to launch a graphical installation.

    If a compatible version of Java is not found on the system, the install program will install the Sun JRE 6 before installing the utility.

By default, the software is installed in %ProgramFiles%\Oracle\Oracle Snap Management Utility.

Configuring the Snap Management Utility Host and Database Host

There are three types of systems that make up an SMU environment: storage appliance, database host, and management (SMU) host. The storage appliance contains the database files, the database host is where the database instances run, and the management host is where SMU runs. It is possible for the database host and management host to be the same.

Default network port settings for all hosts can be reconfigured with the information provided in the following table.

Snap Management Utility requires no further configuration on Oracle Solaris or Oracle Linux database hosts. Microsoft Windows hosts require further configuration, including an HTTPS connection and its required certificate, and Windows Remote Management Service protocol and configuration settings.
IMPORTANT: Only one instance of the Snap Management Utility software should be used to administer a database. Each instance of SMU software stores information about the backups that it creates. This information is not available to other SMU software instances.

Configuring the Network Port Settings

After startup, SMU opens a set of network ports to accept incoming connections from SSH clients, Windows Remote Shell (WinRS) clients, and web browsers. The ports used are user configurable by editing the `smu.conf` file which is located in the `installation/etc` directory or folder. The following table shows the default port settings.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>DEFAULT PORT</th>
<th>CLIENT USAGE NOTES</th>
</tr>
</thead>
</table>
| Windows Remote Shell (HTTPS/encrypted)  | 8001         | Use the `winrs.exe` command with either `-ssl` to specify secure socket layer or `-r` to specify https. The SMU server uses a self-signed certificate. This certificate must be installed in the trusted certificate store on the Windows client host before you can connect to the SMU server. Command examples:  
  - `winrs -r:SMU host FQDN:8001 -u:LOCAL user -ssl smu`  
  - `winrs -r:https://SMU host FQDN:8001 -u:LOCAL user` |
| SSHD Version 2                         | 8002         | Use the `-o "HostKeyAlias <alias>"` option to specify an alias to use. EXAMPLE:  
  - `ssh -l <LOCAL or LDAP user> -p 8002 -o "HostKeyAlias smu" <SMU host>` |
| Web Server (HTTPS/encrypted)           | 8443         | URL: https://<SMU host>:8443/smu The SMU server uses a self-signed certificate. You must accept this certificate before the connection will be allowed. |
Configuring a Windows HTTPS Connection for the Snap Management Utility

In order to use HTTPS connections with the Windows-based host, you must configure the HTTPS listener on the Windows host. An HTTPS listener will require an SSL certificate. The certificate may already be installed on the host or you can install a certificate authority (CA)-signed certificate or generate a self-signed certificate to use.

The following instruction uses the Java 7 keytool command to generate a self-signed certificate for the host.

1. Execute the following command to generate a self-signed certificate:

   \texttt{keytool -genkey -keyalg rsa -keysize 1024 -sigalg sha1withRSA -alias cert -keystore keystore.jks -storepass changeit -keypass changeit -validity 360 -dname "CN=<fully qualified domain name of the host>" -ext KU:true=dS,keyE,dataE -ext EKU:true=serverAuth}

2. Convert the certificate to the correct format:

   \texttt{keytool -importkeystore -srckeystore keystore.jks -srcstorepass changeit -destkeystore cert.p12 -deststoretype PKCS12 deststorepass changeit}

3. Import \texttt{cert.p12} into "Trusted Root Certification Authorities" and "Personal" trust store on the Windows host.

4. Configure the WinRM HTTPS listener:

   \texttt{winrm create winrm/config/listener?Address=*+Transport=HTTPS @{Hostname="<fully qualified domain name of the host>";CertificateThumbprint="<hex thumbprint digits>"}}

5. View the certificate thumbprint by double-clicking the \texttt{host.p12} file and looking at the thumbprint field of the certificate. A thumbprint is 40 hex digits.

6. Verify the listener is configured:

   \texttt{winrm enumerate winrm/config/listener}

Windows Remote Management Protocol and Service Settings for the Windows Database Host

In addition to enabling a listener for Windows hosts, the following Windows Remote Management protocol and service settings must be modified for correct SMU operation:
TABLE 4. RECOMMENDED WINDOWS REMOTE MANAGEMENT PROTOCOL SETTINGS

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFAULT VALUE</th>
<th>SMU RECOMMENDED VALUE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxTimeoutms</td>
<td>60000 (1 minute)</td>
<td>7200000 (2 hours)</td>
<td>Some SMU operations can take a long time to complete. For example, when cloning a database to a different host, SMU may need to recompile schema objects if the host platform changes. This can take an hour or more.</td>
</tr>
<tr>
<td>IdleTimeout</td>
<td>180000 (3 minutes)</td>
<td>7200000 (2 hours)</td>
<td>Increasing the idle timeout for the remote shell on the Windows host allows it to remain open when SMU executes long-running commands. Because SMU alternates issuing commands among the database, storage, and the host, the host can be idle but must remain open.</td>
</tr>
</tbody>
</table>

TABLE 5. RECOMMENDED WINDOWS REMOTE MANAGEMENT SERVICE CONFIGURATION SETTINGS

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFAULT VALUE</th>
<th>SMU RECOMMENDED VALUE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxConcurrentOperationsPerUser</td>
<td>15</td>
<td>1500</td>
<td>While performing operations, SMU executes a greater number of SQL Plus, RMAN, and system commands than the number of commands allowed by default.</td>
</tr>
<tr>
<td>Basic</td>
<td>FALSE</td>
<td>TRUE</td>
<td>This SMU release only supports Basic access authentication.</td>
</tr>
</tbody>
</table>

The following example modifies the Windows Remote Management configuration to meet SMU requirements:

C:\>winrm set winrm/config @{MaxTimeoutms="7200000"}
C:\>winrm set winrm/config/service @{MaxConcurrentOperationsPerUser=1500}
C:\>winrm set winrm/config/service/auth @(Basic="True")
Configuring Host System Name Services Recognized by the SMU Host

While performing its tasks, Snap Management Utility (SMU) logs in to various database hosts and Oracle ZFS Storage appliances. Which systems are used is specified by the accounts that have been added to SMU. Each storage and host account has a hostname property which identifies the name of the system to access. The hostnames or IP addresses used for this property must be resolvable from the management host where SMU is running.

In addition, on database hosts, depending on the database storage type, SMU will examine the system mount table and will resolve the hostnames specified in the resource string for NFS entries. Any hostnames used by the database host or storage appliance must be resolvable from the management host where SMU runs. If may be necessary to add entries to the local hosts file on the management host if there are any hostnames which do not have entries in the environment name service.

Starting and Stopping the Snap Management Utility on Host Systems

The first step in using Snap Management Utility (SMU) is to start the SMU server. SMU has been designed to run continuously on the host upon which it is installed, much like a daemon or network service.

To start the SMU server, execute the SMU launcher script. This script is located in the install bin directory or folder.

**Note:** To start or stop the SMU server, the user must be root. If your server reboots, you will need to restart the Snap Management Utility.

Starting Oracle Snap Management Utility on Linux Hosts

To start Oracle Snap Management Utility on Linux hosts, perform the following command, which will run the SMU server in the background:

```
$ /opt/oracle/smu/bin/smu start
```

To stop the SMU, use the following command:

```
$ /opt/oracle/smu/bin/smu stop
```

To verify that the server is running, use the following command:

```
$ /opt/oracle/smu/bin/smu status
```
Starting Oracle Snap Management Utility on Oracle Solaris Hosts

For Oracle Solaris hosts only, SMU uses Oracle Solaris' Service Management Facility (SMF) service upon startup to run the SMU server in the background.

To start Oracle Snap Management Utility on Oracle Solaris hosts, use the following command.

$ svcadm enable svc:/applicaton/management/smu

To stop the SMU, use the following command:

$ svcadm disable svc:/applicaton/management/smu

To verify that the server is running, use the following command:

$ svcs applicaton/management/smu

Starting Oracle Snap Management Utility on Windows Hosts

To start Oracle Snap Management Utility on Windows hosts, use the following commands.

First register the service with Windows (only need to do this once after installation):

C:\%ProgramFiles%\Oracle\Oracle Snap Management Utility\bin\SmuService /i

To start the service (only need to do this once after installation):

C:\>sc start "Oracle SMU Service"

To stop the service:

C:\>sc stop "Oracle SMU Service"

To check the status of the service:

C:\>sc query "Oracle SMU Service"
To uninstall the service (unregister the service with Windows; only perform if you will be uninstalling the SMU software):

```
C:\>C:\%ProgramFiles%\Oracle\Oracle Snap Management Utility\bin\SmuService /u
```

After the SMU server has successfully started, it creates its files in the SMU server user home directory. Depending on the operating system, the following directory/folder is created:

- For Oracle Linux: `/var/opt/oracle/smu`
- For Oracle Solaris: `/var/opt/ORCLsmu`
- For Windows: `C:\ProgramData\Oracle\Oracle Snap Management Utility`

### Updating the Snap Management Utility on Host Systems

Keep apprised of updates to Snap Management Utility for Oracle Database by visiting My Oracle Support. New releases and minor updates offer the benefits and features of ongoing enhancements to SMU. Instructions for installing these updates is always contained in Read Me files that are included with the update.

For Oracle Solaris hosts, you must uninstall the previous version of SMU before installing the update.

#### Updating Oracle Snap Management Utility on Oracle Solaris Hosts

Use the following commands:

- `# pkgrm ORCLsmu` (removes the existing/old package version)
- `# pkgadd -d ORCLsmu-$VERSION-$RELEASE.all.pkg ORCLsmu` (installs the new package version `$VERSION`, release `$RELEASE`)

#### Updating Oracle Snap Management Utility on Oracle Linux Hosts

Use the following command:

```
# rpm -U oracle-smu-$VERSION-$RELEASE.noarch.rpm (installer upgrade existing software to version $VERSION and release $RELEASE)
```

#### Updating Oracle Snap Management Utility on Windows Hosts

Use the following command:

```
C:\>setup.exe
```
Protecting Oracle Snap Management Utility's Data Files

Depending on the host operating system, SMU uses the following associated directory/folders to store its data files:

Oracle Solaris – /var/opt/ORCLsmu
Linux – /var/opt/oracle/smu
Windows – %PROGRAMDATA%\Oracle\Oracle Snap Management Utility

This directory/folder should be backed up in order to protect this data. Either manually back up the
directory/folder or use standard operating system tools or vendor software to make the backups. To ensure a
consistent backup of the files, the SMU service/daemon should be temporarily stopped for the backup
process.

It is also possible to migrate SMU from one management host to another by taking a backup of the SMU data
on the current management host and restoring the SMU data on a new management host. SMU employs a
Java database to store configuration information of resources that it manages. To protect this core SMU
working data, SMU runtime performs a daily online backup of the Java database. By default, the online
backup of the Java database is scheduled for 23:00 pm. The daily backup schedule can be changed by
modifying the backup.schedule parameter in the $SMU_HOME/etc/smu.conf file. The backup files
are located in the .../backups/mm-dd-yy directory. Use standard operation system commands to delete
the backup files beyond the retention expiration date.

User Permissions Requirements for Accessing Operations

During operations the SMU software accesses both the Oracle Database (database host) and the Oracle ZFS
Storage Appliance (storage system). In order for SMU to access these systems, the software requires that user
accounts be added for these systems. The users specified in these accounts must have the appropriate
permissions or authorizations to perform some privileged commands.

SMU supports three types of host account users: root, Oracle user and delegated user. The following outlines
the permissions that are required by the host account and storage account users.

Host Account User – Must be the root user, or the Oracle user if the Oracle user can do the following:

- Modify the filesystem table (/etc/fstab or /etc/vfstab)
- Create mountpoints under the root directory (/)
- Mount NFS filesystems
• Unmount NFS filesystems
• Scan the SCSI bus for new LUNs

Storage Account User – For detailed information on storage appliance configuration, consult the Oracle ZFS Storage Appliance Administration Guide listed in the References section of this document or access the online help function within the Oracle ZFS Storage Appliance BUI. Users must have the following configuration on the Oracle ZFS Storage Appliance:

• Authorization Levels:
  • Scope: Project and shares
  • Pool: * or specific pool
  • Project: * or specific project
  • Share: * or specific project

• Required Action/Operation Authorizations:
  • changeAccessProps
  • changeGeneralProps
  • clone
  • createShare
  • delete
  • rename
  • rollback
  • takeSnap

With SMU release 1.2, a delegation feature allows designation and use of the sudo tool on Linux and Oracle Solaris database hosts. This delegation to sudo enables a third type of user, called delegated user, who is not root user and not Oracle user. This delegated user can be established with credentials that provide a restricted access for only certain operations that are part of a root user's or Oracle user's permissions. The root user establishes who has sudo privileges.

The term sudo literally means "super user" and "do." See the Glossary for a fuller definition of the sudo tool.
Using SMU Delegation Tools

The SMU delegation tools feature supports the use of sudo on Oracle Linux and Oracle Solaris database hosts. For Oracle users and delegated users, specific database host permissions and authorizations must be configured by the administrator. Using this delegation feature, which is configured as part of the initial application host account setup, the previously listed permissions that are required of root users and must be specifically designated for an Oracle user can be assigned, or delegated, through sudo.

The following host account setup table summarizes permissions and authorizations configurations for Oracle users and delegated users in both single instance and Oracle RAC host accounts.

### TABLE 6. RECOMMENDED HOST ACCOUNT USER PERMISSIONS AND AUTHORIZATIONS CONFIGURATIONS

<table>
<thead>
<tr>
<th>Host Account Type</th>
<th>Host Account User</th>
<th>Permissions and Authorizations Configuration on Linux</th>
<th>Permissions and Authorizations Configuration on Oracle Solaris</th>
</tr>
</thead>
</table>
| Single Instance   | Oracle User       | Set `!requiretty` to sudo user. Sudo privileges include:  
• Using `/usr/bin/find` command for RMAN import feature  
• For NFS:  
  • `mount/umount` NFS filesystems  
  • Create/delete mountpoints under the root directory (/)  
  • (Sudoedit privilege) Modify the filesystem table (/etc/fstab)  
• For ASM:  
  • Scan the SCSI bus for new LUNS (`/usr/bin/scsi-rescan -r`)  
  • Trigger and settle udev events  
  • (Sudoedit privilege) Modify the udev rules (/etc/udev/rules/*.rules) |
|                   | Delegated User    | Group Memberships (typically, same as Oracle User's):  
• primary group = OSDBA (default dba)  
• secondary group = Oracle Install Group (default oinstall)  
• if ASM is used, also add ASMADM and ASMDBA groups.  
Requires user home directory. Sudo privilege to run `$ORACLE_HOME/bin/orapwd` as the user. |
|                   |                   | Group Memberships (typically, same as Oracle User's):  
• primary group = OSDBA (default dba)  
• secondary group = Oracle Install Group (default oinstall)  
• if ASM is used, also add ASMADM and ASMDBA groups.  
Requires user home directory. Sudo privilege to run `$ORACLE_HOME/bin/orapwd` as the user. |
<table>
<thead>
<tr>
<th>Host Account Type</th>
<th>Host Account User</th>
<th>Permissions and Authorizations Configuration on Linux</th>
<th>Permissions and Authorizations Configuration on Oracle Solaris</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Oracle User with the ORACLE_HOME environment variable set.</td>
<td>Oracle User with the ORACLE_HOME environment variable set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The ORACLE_HOME environment variable identifies the base directory for the Oracle home where the orapwd command is located.</td>
<td>The ORACLE_HOME environment variable identifies the base directory for the Oracle home where the orapwd command is located.</td>
</tr>
<tr>
<td>Oracle RAC</td>
<td>Delegated User</td>
<td>User’s single instance host requirements must be satisfied plus:</td>
<td>User’s single instance host requirements must be satisfied plus:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User must exist on all RAC nodes</td>
<td>User must exist on all RAC nodes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User’s configuration such as user id and group must be the same on all RAC nodes</td>
<td>User’s configuration such as user id and group must be the same on all RAC nodes</td>
</tr>
</tbody>
</table>

The following table lists the SMU command summary for sudo policy files for the Linux and Oracle Solaris operating systems:

**TABLE 7. SUDO POLICY FILE SMU COMMAND SUMMARY**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>NFS Clone</th>
<th>ASM Clone</th>
<th>Import RMAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>/bin/mount, /bin/umount, /bin/mkdir, /bin/rmdir, sudoedit /etc/fstab, /bin/rm, /usr/bin/install</td>
<td>/usr/bin/scsi-rescan, /sbin/scsi_id, /bin/mount, /bin/umount, /bin/mkdir, /bin/rmdir, sudoedit /etc/udev/rules.d/99-smu.rules, /sbin/udevadm trigger (OEL6), /sbin/udevadm settle (OEL6), /sbin/udevsettle (OEL5), $ORACLE_HOME/bin/orapwd (delegated user)</td>
<td>/bin/mount, /bin/umount, /bin/mkdir, /bin/rmdir, sudoedit /etc/fstab, /usr/bin/find, /bin/rm, /usr/bin/install $ORACLE_HOME/bin/orapwd (delegated user)</td>
</tr>
<tr>
<td>Oracle Solaris</td>
<td>/usr/sbin/mount, /usr/sbin/umount, /bin/mkdir, /bin/rmdir, sudoedit /etc/vfstab, /bin/rm, /usr/sbin/install</td>
<td>/usr/sbin/disks, /usr/sbin/mount, /usr/sbin/umount, /bin/mkdir, /bin/rmdir, /bin/chmod, /bin/chown, /bin/rm</td>
<td>/usr/sbin/mount, /usr/sbin/umount, /bin/mkdir, /bin/rmdir, sudoedit /etc/vfstab, /usr/bin/find, /bin/rm, /usr/sbin/install $ORACLE_HOME/bin/orapwd (delegated user)</td>
</tr>
</tbody>
</table>
Sample sudo policy file configuration format (/etc/sudoers)

Defaults <user> !requiretty
Defaults    env_keep += "ORACLE_HOME"
Cmnd_Alias SMU = /bin/mount, /bin/umount, /bin/mkdir, /bin/rmdir, /bin/rm, sudoedit /etc/fstab, /usr/bin/install, /u01/app/oracle/product/11.2.0/dbhome_1/bin/orapwd ...

<user> ALL=(root, oracle) NOPASSWD:SMU

Be sure to consider your organization’s security policies or standard operating procedures when assigning permissions as described in these requirements.

IMPORTANT: The sudo command/utility is standard on Linux 5, Linux 6, and Oracle Solaris 11. It is not standard, however, for Oracle Solaris 10 clients, and administrators must obtain it from a third-party location. Recommended locations are the SUDO web site at www.sudo.ws or the Solaris Companion CD at sunfreeware.com.

Accessing the User Interfaces

SMU provides two user interfaces: a browser user interface (BUI) and a command-line interface (CLI). The command-line interface can be accessed using SSH or WinRS clients. The browser user interface can be accessed using any standard web browser.

Command-Line Interface

The SMU command-line interface can be accessed using standard remote shell commands: the ssh command on UNIX hosts, and the winrs.exe command on Windows hosts.

Accessing the Command-Line Interface Using SSH

Secure Shell is the standard for remote shell access on UNIX hosts. SMU embeds an SSHDv2 server to allow easy access to the SMU CLI from UNIX environments.

To access the command-line interface using SSH, type the following command:

$ ssh -l <username> -p <port> -o "HostKeyAlias <alias>" <hostname>

You can specify a local or LDAP user that exists in the SMU database. For port, use the port number that is specified in the smu.conf file. The HostKeyAlias option is used to create and/or reference a separate record in the SSH $HOME/.ssh/known_hosts file. By default the ssh command uses the hostname as the alias. By specifying a separate alias, you are able to have two separate records in the client file: one for the host and one for the SMU server.
Accessing the Command-Line Interface Using WinRS

Windows Remote Shell (WinRS) is a standard command for accessing other Windows systems remotely. For more information on Windows Remote Shell, please consult the Microsoft Windows documentation at: http://technet.microsoft.com. SMU embeds a WinRS server for easy access to the SMU CLI from Windows environments.

To access the command-line interface using encrypted WinRS, type the following command:

```
C:>winrs -r:<hostname>:<port> -u:<username> -ssl smu
```

Only local SMU users are supported using this access method. The port should be the port number that is specified in the `smu.conf` file for WinRS. The command argument must be `smu`. This indicates that the SMU command shell should be executed.

Authenticating with WinRS

The SMU WinRS server only supports Basic authentication. You must configure the following `winrm/config/client` properties to access the SMU server:

```
c:\>winrm set winrm/config/client @{AllowUnencrypted="true"}
c:\>winrm set winrm/config/client/auth @{Basic="true"}
c:\>winrm set winrm/config/client @{TrustedHosts="<hostname>"}
```

You must also ensure that the LAN Manager authentication level will support the Microsoft security protocols LAN Manager and NT LAN Manager (designated as LM & NTLM), and use NTLMv2 session security if negotiated.

1. Open the Local Security Policy.
2. From a command prompt, enter `secpol.msc`.
5. Double-click Network security: LAN Manager authentication level.
6. Select Send LM & NTLM – Use NTLMv2 session security if negotiated from the pull-down menu.
7. Click OK.
Note that you will have to add the SMU service self-signed certificate to the trusted certificate store on your Windows host before connecting. To obtain the SMU service self-signed certificate, perform the following steps. Instructions for both SSH and web browser sessions are shown.

Using SSH:

1. Log in to SMU.
2. Enter `certs get all`.
3. Copy the encoded certificate (encoded text starts with "----BEGIN CERTIFICATE----" and ends with "----END CERTIFICATE----") and paste it into a file.
4. Save the file, using the suggested file extension `.cer`, which is the standard file extension for X.509 certificates.
5. Right-click on the certificate file from Internet Explorer and select "Install Certificate".
6. Make sure the certificate is installed into the "Trusted Root Certificate Authorities" certificate store.

Using your web browser:

1. Point your browser to URL `https://<SMU Host>:8443`.
2. You should be presented with the "Untrusted Connection" page, where you will select the following:
   - Click the Add Exception... button.
   - Click the View button.
   - Click the Details tab.
   - Click the Export button.
3. Save the certificate to a file. The file extension `.cer` is automatically used.
4. Right-click on the certificate file from Explorer and select "Install Certificate".
5. Make sure the certificate is installed into the "Trusted Root Certificate Authorities" certificate store.

Accessing and Authenticating Using the Browser User Interface

The SMU browser user interface is accessed using a standard web browser. For detailed listings of supported browsers and recommended settings information, see: [http://jdevadf.oracle.com/ADF-RichClient-Demo/docs/release.html#SupportedPlatforms](http://jdevadf.oracle.com/ADF-RichClient-Demo/docs/release.html#SupportedPlatforms).
The following table lists standard supported web browsers.

**TABLE 8. SUPPORTED WEB BROWSERS**

<table>
<thead>
<tr>
<th>WEB BROWSER</th>
<th>SUPPORTED VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>2.x through 13+</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>7, 8, 9</td>
</tr>
<tr>
<td>Safari</td>
<td>3.1.2, 4, 5</td>
</tr>
</tbody>
</table>

To access the encrypted SMU web application, use the following URL:

https://<hostname>:<port>/smu

The hostname is the hostname or IP address of the host upon which SMU is running. The port number is the HTTPS port (encrypted application) specified in the smu.conf file. The default port is 8443.

The SMU web server uses a self-signed certificate. You must accept the certificate the first time you access the SMU web server using HTTPS.

Once you are connected to the SMU BUI, you will be presented with the SMU login page. To log in to the SMU BUI, enter your SMU user and password. For initial access to the SMU BUI, you can use the user name admin, then the default password changeit. Once you log in to the SMU BUI, you should be able to change the password on the User tab of the Administrations panel.

**Navigating the Browser User Interface**

The Snap Management Utility for Oracle Database provides an easy-to-use Browser User Interface (BUI) for managing its operations. Figure 1 shows the basic BUI layout, in which the main window is divided into a Workgroup navigation tree at left, a main or center detailed display for the selected Workgroup item and, at bottom, a Tasks screen which displays details of tasks in process or previously executed.
On the upper right side of the BUI, you can access links for general information about the installed Snap Management Utility (the link labeled About, which provides the SMU version), the online help (Help), which contains a quick-reference form of the user guide information contained in this document, the accessibility preferences (the link labeled Accessibility), the logged-in user (“admin” in this example), and the SMU logout.

Clicking on the Accessibility link generates the Accessibility Preferences dialog window, as seen in figure 2. From this window, you can choose display preferences so that the Snap Management Utility BUI will optimize for the selected accessibility preference.
The Tasks screen provides important details for any operations initiated in SMU. Actions such as deleting or canceling a task, or changing or refreshing the display are managed with pull-down menus and selectable icons. On the right side of the Tasks display, icons provide sort options for the Tasks display. Mouse over each of the icons for a text descriptor of the icon's sort parameter. (Note that any task failures have purposefully been shown in this panel for examples.)

The Workgroup panel's navigation tree is subdivided into Applications, Accounts, Activity Logs, and Administration. For each of the left-sided categories under Workgroup, the Actions and View pull-down menus, as well as the corresponding icons, will change for the permissible actions within that category.

In figure 3 in the Applications view, the Actions pull-down menu allows you to add, modify, remove, or test (check on the accessibility of) an application, as well as import (clone) an RMAN image and deprovision a cloned application. Selecting the corresponding icons to the right of the Actions and View pull-down menus also accomplishes the same actions. Mouse over each of the icons for a text descriptor of its function.
The main Applications panel lists a summary subtree of clones associated with a particular application, so that the relationships of source-target is easily viewed from this window. The clone's system identifier (SID) next to Type identifies the clone's characteristic, such as split clone or thin clone, and icons and prefixes in the database instance name duplicate this information. The Workgroup window's navigation tree can expand in the Applications category to show this information and subordinate relationships as well. You can expand and collapse the Workgroup navigation tree by selecting the directional arrow to the left side of the main/center display.

For a complete list of the BUI icons and their meanings, see Appendix C.

When you select a listed application, the main panel display changes to feature tabs for Snap Backups, where all the backup and clone operations are accessed, Schedules, where timeframes for scheduled operations are set, and Account Settings, which displays and accepts modifications for Application, Application Host, and Storage information.

The following sections provide basic information and procedures for common tasks within the four workgroup, or feature, categories.

Managing Accounts Using the BUI

SMU accomplishes snap backup operations by coordinating functions of the application (database), the application host where the application is running, and the storage system where the application’s data resides. The accounts of applications are managed on the Applications page while the accounts of application hosts or storage systems are managed on the Accounts page.

An application account is associated with an application host account and a storage system account. An application host account and a storage system account can be associated to many application accounts. Because of this relationship, the application host account and the storage system account must be created before an application account associated with them is created. An application host account or a storage system account cannot be deleted while they are in use by an application account.

**Important:** Be sure to review the section "User Permission Requirements for Accessing Operations" in this document for further information on accounts. Further information on delegation is also included in that section.

The SMU BUI's Accounts panel, seen in Figure 4, contains tabs for the registered host accounts and storage accounts. These accounts must be created before taking any snap backups.

Note that the name of an account, including host, storage, and application accounts, must be unique within an SMU instance. An account name consists of alphanumeric characters or one of these permissible special
characters: _ (underscore), . (period), @, and - (hyphen). An account name may not start with a number. The maximum account name length is 64 characters.

Selecting the Host Accounts tab lists all the accounts created for connecting to the hosts. The displayed columns under Host Accounts show the following items:

Account (Name) – Unique name of the account to access the application host.

Host – Domain name or IP address of the application host.

Type – Indicates whether the application host is a UNIX-based (Oracle Linux or Oracle Solaris) or a Windows application host.

Protocol – Either SSH2 or WINRS.

Port – Port number used to connect to the application host using the protocol designated in the Protocol field.

Delegate – Either NONE or SUDO.

User – User name to use to establish the connection to the application host.

Applications – Number of applications assigned under the selected account. Note that this number is a hyperlink which, when selected, produces a pop-up application list showing the associated application names.

![Figure 4. Application Host Accounts tab listing under Accounts in SMU BUI](image-url)
Similarly to the Application Host Accounts tab, the Storage Accounts tab lists all the accounts created for connecting to the available Oracle ZFS Storage Appliance(s). The provided column information, as seen in figure 5, includes:

Account (Name) – Unique name of the account to access the storage system (Oracle ZFS Storage Appliance).
Storage – Domain name or IP address of the Oracle ZFS Storage Appliance.
Type – The type of storage system. Type is ZFS Storage Appliance by default.
Port – Port number used to connect to the SSH interface for the Oracle ZFS Storage Appliance.
User – User name to use to establish connection to the Oracle ZFS Storage Appliance.
Applications – Number of applications assigned under the selected account.

Figure 5. Listing for Storage Accounts tab

From the Accounts BUI page, you can easily perform the following tasks under the Application Host Accounts and Storage Accounts tabs by following the provided steps.
Adding a new host account

1. Selecting the Application Host Accounts tab, choose Actions, and then Add.
2. Provide entries for the following: a unique name for Account, Host Name, Protocol (either SSH2 or WINRS), Port, Delegation, User, Password, then Confirm password.
3. Click on OK.

Modifying a host account

1. From the list of application host accounts, select and highlight a row (host account) to edit.
2. Click on Actions, then Modify.
3. Make any needed changes to the fields displayed in the Modify Application Host Account window that displays and click OK.

Deleting a host account

Note that when an application host account is in use by an application, the host account cannot be deleted. Attempting to delete a host account in use results in an error.

1. From the list of application host accounts, select and highlight the row (host account) to delete.
2. Click on Actions, then Remove.
3. A warning message displays, indicating that deleting a host account will disable snap backup operations on the applications running on the host. Click on Yes to confirm that you want to delete this host account.

Adding a new storage account

For clustered storage: be sure to reference the section "Special Considerations with Clustered Systems" at the beginning of this document.

1. Selecting the Storage Accounts tab, choose Actions, and then Add.
2. Provide entries for the following: a unique Account name, Storage Name, Type (no entry required; only Oracle ZFS Storage Appliance is supported and automatically populates), Port number, User name, Password, then Confirm Password.

3. Click on OK.

Modifying a storage account

1. From the list of storage accounts, select and highlight a row (storage account entry) to edit.
2. Click on Actions, then Modify.
3. Make any needed changes to the fields in the Modify Storage Account window and click OK.

Deleting a storage account

Note: SMU will not delete a storage account unless the associated application account has already been deprovisioned or deleted.

1. From the list of storage accounts, select and highlight the row (storage account) to delete.
2. Click on Actions, then Remove.
3. A warning message displays, indicating that deleting a storage account will disable snap backup operations on the applications that consume the storage. Click on Yes to confirm that you want to delete this storage account.

Managing Applications Using the BUI

Figure 1 shows the display for the selection Applications, with the pull-down menu for choosing options for Views. Basic information such as the application's host account, storage account, and whether it has a backup schedule or existing snap backups, is readily seen for the applications/databases registered. The columns list the following information:

Name – Unique name of the account to access the application (database) running on the application host.
Type – Type of the database. Currently, only Oracle Database is supported.
SID/SID Prefix – The database system identifier (SID) or SID prefix without node index number in case the database is a Real Application Cluster (RAC) or RAC One Node. Identifies the characteristic of a clone.

Cluster – Indicates whether the database host is a clustered system or not (single instance).

Backups – Indicates the number of existing copies of the application (database) SMU has already taken.

Schedules – Indicates the number of existing snap backup schedules configured for the application (database).

Clones – Indicates the number of all clones created from this application (database).

Host Account – Account name of the application host.

Storage Account – Account name of the storage system.

**Important:** Note the test icon – A clickable icon that will check validation of application credentials, appearing in the Actions and View line's list of icons. Be sure when you add or modify accounts to use the test icon to validate the changes.

From this Application BUI page, you can easily perform the following tasks by following the provided steps.

**Enrolling a new application for snap backups**

Note that an application host account and a storage system account must already exist so that an application account can use them when the application account is created. If you have not created the application host account and the storage system account to use with the application account, you can create them using the instructions in the "Adding a new host account" and the "Adding a new storage account" sections.

1. From the left-side Workgroup panel/navigation tree, click on Applications.

2. Click on Actions, then Add. The Add Application Account dialog window is displayed.

3. Fill in entries for application account Name, Type (no entry required; automatically populates with Oracle Database), SID/SID Prefix, Listener Port, checkbox for Cluster Database, User (populates automatically with default sys user), Password (password of the sys user), Confirm Password, and drop-down windows for Host Account and Storage Account.

   Note that SID Prefix without RAC node index must be specified for the SID/SID Prefix field in case of RAC or RAC One Node database. In addition, the Cluster Database checkbox must be checked for RAC or RAC One Node database.

4. Click OK. The newly enrolled application appears in the Application Table and also under Applications listed on the left side of the panel.
Modifying an application account

1. From the navigation tree, select Applications. This shows all the applications previously enrolled in SMU.
2. From the list of enrolled applications, select and highlight a row (application) to edit.
3. Click on Actions, then Modify.
4. Make any needed changes in the fields displayed in the Modify Application Account window and click OK.

Removing an application

Note that you cannot delete an application account when the application has snap backups or backup schedules configured on it. You should delete all snap backups and backup schedules prior to deleting the application. Attempting to delete an application when the application has snap backups or backup schedules results in an error.

1. From the navigation tree, select Applications. This shows all the applications previously enrolled in SMU.
2. From the list of enrolled applications, select and highlight a row (application) you want to remove.
3. Click on Actions, then Remove.
4. A warning message displays, indicating that deleting an application will disable snap backup configuration for the application. Click on OK to affirm that you want to remove this row/application.

Testing an application

Initiating the test operation will validate the database instance functionality. Highlight the application you wish to test, then select Test from the pull-down Actions menu. Note that this operation, once selected, cannot be canceled.

Importing an RMAN backup image

Note that as part of the RMAN Backup Image import operations, an application account for the clone application is created. A new node for the clone application appears under the Applications node of the navigation tree. The application summary table also lists the newly created clone application. If an RMAN Backup Image import operation fails, the clone application node is removed upon the page being refreshed in the next polling cycle. You can press the Refresh button to make sure you have the latest updated application summary.

Important: If you intend to take online backups of clones created by importing an RMAN backup, the backed-up datafiles and archived logs must be in separate backup shares. This setup can be accomplished by
allocating files to different RMAN channels. The following RMAN run block script employs the channel parameter to separate the datafiles and archived logs and should be run:

```
connect target /
configure controlfile autobackup on;
run {
  # this undoc command will ensure that no autobackup is generated
  # at the end of this script
  set nocfau;
  allocate channel ch01 device type disk format '/rman01/%U';
  allocate channel ch02 device type disk format '/rman02/%U';
  backup as copy database channel ch01 plus archivelog channel ch02;
  backup as copy current controlfile channel ch01;
}
```

**IMPORTANT:** Currently, importing an RMAN backup image from a RAC One Node configuration is not supported.

1. From the navigation tree, select Applications. This shows all the applications previously enrolled in SMU.

To clone from an RMAN image copy that is stored in multiple shares, you can specify one or more share mountpoints, separated by commas, as the value of the RMAN Image path, which is the list of filesystem shares in which the backup is contained. Shares are identified by their mountpoint property (a path like `/export/backup`).

Note that for multithread cases, SMU will check the heads automatically as it searches for the specified shares. Users can choose either head of a dual-head system.

2. Click on Actions, then Import RMAN Image. The Import RMAN Backup Image wizard's dialog windows will display.

3. Required entries are prompted in two steps: locating the RMAN image and specifying the database account information. Choose the RMAN image's storage location(s) from a drop-down list, enter a value for RMAN Image Path or, in the case of multiple-share storage locations, provide a comma-separated list of values, and click on Next. The step 2 dialog window requires the following to create the new database account for the imported RMAN backup image:

- **Host** – Choose from the drop-down list displaying all registered host accounts.
- **Account Name** – In which to create the RMAN clone database.
• SID/SID Prefix – If the clone is a single instance, use the specified SID as is. If the clone is a RAC (cluster), the specified SID prefix accompanies the index numbers used to assign the SID to members of the RAC.

• Listener Port – The port number of SQL*Net listener. The default setting is 1521, but it can be changed.

• Cluster checkbox – Check if applicable (RAC).

• Database Name – Global name of the clone database.

• Database Home – Path to the Oracle Database software home.

• User – Automatically populated with sys.

• (DB) Password

• Confirm Password

4. Click Finish. The newly enrolled application should appear in the Application table as well as under the left-side Workgroup panel, under Applications.

Note: Selecting Actions and Refresh will reload the BUI page so that the latest updated Applications information appears onscreen.

Deprovisioning an application (clone only)

Note that only clones created from SMU can be deprovisioned. Deprovisioning removes all artifacts of the clone as well as the application account for the clone. Once a deprovision operation gets started, it cannot be undone. Canceling a deprovisioning operation may leave the clone in an unknown state. SMU should refresh the BUI page when the deprovision operation has completed and the next polling cycle is hit. You can press the Refresh button to make sure you have the latest updated application summary.

1. From the navigation tree, select Applications. This shows all the applications previously enrolled in SMU.

2. From the list of enrolled applications, select and highlight a row (application) to deprovision.

3. Click on Actions, then Deprovision.

4. A warning message displays, indicating that deprovisioning deletes a clone from the host and detaches the backend storage. You are prompted to fill in the clone name that you wish to deprovision. Provide the clone name and click on OK to affirm that you want to deprovision this application from the host and storage accounts.
Managing Administration Using the BUI

All user administration activities can be performed in the Administration screen. Administration is the last category selection under Workgroup on the left side of the screen. The Administration screen contains three tabs: Users, Notification, and General Settings.

Only the Snap Management Utility administrator has privileges to add, modify, or remove other users’ access to the SMU. Clicking on the Users tab brings up a table that shows all the existing users of the SMU. The following columns are displayed in the table, as seen in figure 6:

User – The user name is used for login to the SMU.

Type – Indicates whether the user is a local or LDAP user.

Full Name – The actual name of the user.

Directory Server – The Directory Server name that holds this user information.

Directory – For LDAP users, the location where their user details reside on the Directory Server (the LDAP search base for the user authentication).

The following BUI instructions provide details on adding, modifying, or deleting user entries in the Snap Management Utility.

Adding a new user from the Users tab

1. Selecting the Users tab, choose Actions, and then Add User.

2. Choose either the Local User or LDAP User tab.

3. Provide entries for the following for Local User: User, Full Name, Password, then Confirm Password. For LDAP User, provide the User, and user's Directory Server and Directory.

4. Click on OK.
Modifying a user entry from the Users tab

1. From the list of users, select and highlight a row (user) to edit.
2. Click on Actions, then Modify.
3. Make the needed changes to the fields displayed in the Modify User dialog window and click OK to commit to the changes.

Deleting (Remove) a user from the Users tab

1. From the list of user accounts, select and highlight the row (user) to delete (remove).
2. Click on Actions, then Remove.
3. As indicated in the warning message that displays, once the user entry is deleted, the user will no longer be able to log in to the SMU. Click on OK to confirm that you want to remove this user.

SMU allows users to subscribe to notices for any important events that might occur while the SMU is running the tasks initiated by the users. For example, users can subscribe to receive email alerts when any SMU task is cancelled or failed.

The display for Administration’s Notification Tab presents two columns, as seen in figure 7: a list of all the events the users subscribed to (Subscribed Events) and the email addresses to which notices are sent (Email Address).

The following instructions for adding, modifying, and removing notifications are similar to the Users add, modify, and remove instructions.
Adding a new notification subscription

1. Selecting the Notification tab, choose Actions, and then Add.

2. Provide entries for the following: Event Types (Choose among the options All, Task Cancelled, and Task Failed. Selecting All will initiate email notices for all SMU events; currently only Task Cancelled and Task Failed events are supported.), and Email (to which the notification is sent).

3. Click on OK.

Modifying a notification subscription from the Notification tab

1. From the list of notification subscriptions, select and highlight a row (subscription) to edit.

2. Click on Actions, then Modify. The dialog box ‘Modify Notification Subscription’ is displayed.

3. Modify the details to the following elements:
   - Event Types: Currently SMU can send the email alerts when a task is canceled or when it is failed. Selecting the “All” checkbox will let you receive all supported notification events from SMU. You can individually select subscription to either “Task Cancelled” or “Task Failed” using the checkboxes. Unselecting the checkboxes removes the subscription to those events.
   - Email: Change the email address to which notices are sent.

4. Make the needed changes to the fields and click OK.

Deleting a notification subscription from the Notifications tab

1. From the list of notification subscriptions, select and highlight the row (notification subscription) to delete.

2. Click on Actions, then Remove.

3. Click on OK to confirm that you want to remove this notification subscription.

The changes to Notifications will become effective immediately and the user will start (or stop, if that is the case) receiving the subscribed notifications whenever they occur on SMU.
Managing status polling, and task and activity log displays in the General Settings tab

SMU operates using asynchronous-based commands. For example, when SMU creates a backup or a clone of a database, it automatically determines the dependent mount points and the corresponding LUNS and shares on the Oracle ZFS Storage Appliance and initiates the backup process on the Oracle ZFS Storage Appliance. Depending upon the size of the database to be copied, the operation can take a considerable amount of time. In order to allow other operations on the SMU, every user-initiated activity related to the database backup is designed to work asynchronously. The moment any such operation is started, the task is listed in the Tasks panel at the bottom of the SMU BUI. Then onwards, the SMU BUI periodically polls the SMU server and/or Oracle ZFS Storage Appliances to check the status (or state) of the initiated tasks and update their status information in the Tasks panel.

In the General Settings tab’s display, as seen in figure 8, users can use the Browser Auto-Refresh panel to set the poll intervals for their own individual settings. The general settings are stored and applied across the SMU logins of that particular user. The following fields are used:

Disable Polling checkbox – Checking and unchecking this box will, respectively, disable and enable the polling process.

Polling Interval (secs) – Indicates how often the SMU BUI should poll the SMU server and the Oracle ZFS Storage Appliances to determine the running status of the task. A user can enter a new value either by typing the value or using the increment/decrement arrows.

Polling Timeout (secs) – Indicates the amount of time in seconds to pause polling when the user is not actively using the SMU BUI. The polling timeout allows the user login session to expire when the user does not use the BUI for awhile. The actual user login session expiration time is determined by adding the polling timeout to the SMU BUI session timeout (30 minutes). Users can enter a new value either by typing the value or using the increment/decrement arrows.

Once the Update button is selected, the new changes take effect immediately.

IMPORTANT: If SMU is managing a heavy load of items and the BUI auto-refresh polling interval setting is too short, the BUI may keep reloading a page before it can render it. This issue may block navigation to the General Settings panel and, thus, the ability to change the auto-refresh setting.

To address this, disable the auto-refresh BUI process by changing the `bui.autorefresh.disable` parameter to `true` in the `$SMU_HOME/etc/smu.conf` file. After changing the parameter, restart SMU, then navigate to the General Settings tab and adjust the auto-refresh polling interval to a larger span.

The next panel, Task Monitoring, provides control over the viewable number of tasks in the Tasks window display using the Maximum Task Display settings. Either enter the desired maximum line count or use the increment/decrement arrows to change this setting to customize this display for your particular screen display parameters.
Similar display controls for number of rows per page can be set in the last two panels, Snap Backups and Activity Logs.

![Oracle Snap Management Utility](image)

**Figure 8.** Polling frequency and various maximum line display settings under Administration and General Settings tab

**Operating and Managing Snap Backups in the BUI**

Backups can be created manually or automatically. Automatic backups can be scheduled to occur on a recurring basis. Automatic backups can also have a retention policy setting the number of backups to retain at a time.

Two types of backups are supported. Offline backups are backups taken when the database is shut down. The software will shut down the database temporarily and then restart it after taking the snap backups. Online backups are backups taken when the database is placed into backup mode while remaining online. Online backups snapshot the database shares in a particular order.

In the BUI, indicate which application to target for a snap backup by clicking on Applications on the left-side panel under Workgroup panel, then selecting the application from the list by clicking on it. This will bring up another panel in the middle of the screen with three tabs: Snap Backups, Schedules, and Account Settings, as seen in figure 9.
The Snap Backups tab provides a table displaying the list of snap backups taken for the selected application. The table includes the following details:

Name – The unique name for the snap backup that will be taken. The name consists of alphanumeric characters, with a maximum length of 64 characters, and including permissible special characters (only "_" [underscore] and "." [period]). Snap backup names must not begin with a number.

Type – Indicates the snap backup types: Online or Offline.

Mode – Indicates whether the snap backup was scheduled for automatic execution or manually initiated.

Creation Time – The time when the snap backup was taken.

Clones – Number of clones associated with this snap backup. The number is a hyperlink that, once selected, produces a separate pop-up window showing the list of clones and their associated clone account names. Each clone account name is also a hyperlink which, when selected, produces the backup information window for the selected clone account.

On the right side of the display, scroll arrows for up, down, first, last, previous and next task items are selectable. The Jump To tab, when selected, presents a dialog box to choose a task ID for display.

The following instructions include basic operations for taking and managing snap backups and clones in the Snap Management Utility BUI.
Creating a new snap backup

1. Click on Actions, then select Backup. Figure 10 shows the possible actions, including Backup, in the Actions pull-down window.

2. A new dialog window pops up, as seen in figure 11. Enter a unique name in the Name field for the snap backup you are creating.

3. Select the Type from the drop-down list for the snap backup you want to create: Offline or Online.

4. Click OK.
You will see a task in the Tasks Panel at the bottom of the screen that has been created for taking this snap backup. If the snap backup succeeds, it displays in the table under the Snap Backup tab, and the corresponding task in the Tasks panel displays a green check in the checkbox in the Status column. If the snap backup task fails, the Output column indicates a red crossmark (x). Clicking on the status indicator for the particular operation provides a task output popup display which, in the case of a failed status, includes the reason for the failure within the detailed task output.

Figure 12 shows a series of successful operations, including backups, displayed in the Tasks pane.

Figure 12. Listing of backup operation results in the Tasks window

Renaming a snap backup entry

1. From the list of displayed snap backup entries, select and highlight the row (backup) that you want to rename.
2. Click on Actions and Rename.
3. A dialog window labeled Rename Snap Backup will be displayed. Provide the new name in the Name field.
4. Click on OK.

**IMPORTANT**: If a snap backup has been cloned, the rename of the snap backup cannot be performed. SMU will block the rename operation on a snap backup that has clones.

Cloning a snap backup entry

SMU can be used to clone a database and create a new primary database. This database is created using Oracle ZFS Storage Appliance clone technology. ZFS clones are thin-cloned datasets that share common data blocks with the original dataset. This allows the clones to be space efficient and created very quickly.

SMU supports cloning both single instance and RAC instance databases, which are differentiated in the `cluster_database` property setting in their respective application accounts. When the property is set to true, the application account represents a clustered (RAC) database. When the property is set to false, the application account represents a single instance database. When selecting the target account in the cloning dialog window, you do not need to explicitly specify (define again) whether the selected target is a single instance or RAC instance.
Important: If you are cloning an instance of Oracle Database that uses its transparent data encryption (TDE) feature, you must manually copy the encrypted database’s wallet file to the target host, modify the sqlnet.ora file to point to the wallet file, then restart the clone. See Appendix D: Cloning Wallet Files for an Encrypted Database of this document for further information.

Ensure that the targeted host has adequate resources, including shared memory, to handle the addition of another database.

In order to create a database clone from a snap backup on another host, the target host must meet certain requirements:

- The Oracle user must have the same uid/gid as the source database host, since cloning a snap produces a new share with the same files and ownership as the original share.
- If the Oracle home is different on the target host, you must specify the Oracle home as a clone option. By default, SMU uses the same Oracle home setting as the source database.
- The Oracle Database software must be the same version as on the source database host. SMU does not perform downgrades or upgrades during the clone operation.

If dNFS is desired for the clone database, it must be configured in the target Oracle home before the clone operation is performed.

Use the following steps to clone a database.

1. From the navigation tree, click “Applications” and click on the application for which a snap backup(s) has already been taken.

2. From the list of the snap backup entries that are displayed, select and highlight the row (snap backup) that you want to clone.

3. Click on Actions and Clone. Enter the required information in the pop-up dialog window called Create Primary Clone, as shown in figure 13. The required field entries are:

- Host Account – Choose from the drop-down list displaying all registered host accounts.
- Application Name – In which to create the clone database.
- Type – Automatically populates (Oracle Database is the default.)
- SID/SID Prefix – If the clone is a single instance, use the specified SID as is. If the clone is a RAC (cluster), the specified SID prefix accompanies the index numbers used to assign the SID to members of the RAC.
• Listener Port – The port number of SQL*Net listener. The default setting is 1521, but it can be changed.
• Cluster checkbox – Check if applicable (RAC).
• Database Name – Global name of the clone database.
• Database Home – Path to the Oracle Database software home.
• User – Automatically populated with sys.
• Password
• Confirm Password

Figure 13. Clone Snap Backup dialog window

4. Upon completing the required fields, select Next. The Primary Clone Summary window appears with details on the clone for verification. Selecting Finish starts the clone process.

In the Task Panel at the bottom of the screen, you will see the task that has been created for cloning this snap backup. If the cloning succeeds, the BUI displays the account name of the cloned application (database) in the navigation tree under the Applications node, and in the table under the Snap Backup tab. The corresponding task in the Task panel displays a green check in the Status column. If the cloning task fails, the Status column
displays a red cross-check (×). Clicking on the status indicator icon produces a detailed Task Output display which, in the case of a failure, indicates the reason for the failure.

Rolling back (restoring) a snap backup

SMU can be used to restore a database from an on-disk backup. The restore is accomplished using ZFS rollback technology. Rollbacks allow you to revert a dataset back to a point in time without having to copy or delete any data.

You can only restore a database to the specified backup if there are no database clones made from any newer backups of that database. Since backups are based on ZFS snapshots, restoring to a snap backup automatically destroys any newer snap backups.

Figure 14 shows a selected Restore operation. Choosing the reverse arrow icon, listed horizontally next to the Actions and View menus, will also initiate the operation.

Figure 14. Choosing Restore to roll back to the previous selected database snap backup

**Important:** This step will revert all the active data, and any more recent snap backups or clones will be deleted. This operation cannot be undone.

1. From the list of applications, select and highlight the application in which you want to perform a rollback.

2. A list of existing snap backups for the selected application will be displayed. Select the snap backup you wish to restore (roll back to) by clicking on it.

3. Click on Actions and Restore.

4. A warning reminder that all existing snap backups and clones that occurred after the selected restore target will be deleted pops up. To execute the restore, select OK.
Deleting a snap backup entry

**Important:** You can only delete a backup if it does not have any dependent clones. When performing a delete task, SMU checks the backup to see if any clones were made from it and the clones are still active. If there are active clones, SMU will fail the task and not allow the backup to be deleted.

1. From the list of the snap backup entries that are displayed, select and highlight the row that you want to delete.
2. Click on Actions and Delete.
3. A warning message indicating all data within the snap backup will be lost, and the operation cannot be undone, appears. Click on OK to confirm the delete operation on this row.

Running Simultaneous Snap Operations

SMU allows snap operations on different applications to run in parallel, so that you can take snap backups on multiple applications or create more than one clone at the same time. SMU performs snap operations on the same application sequentially in order to preserve the dependencies among snap operations and resources. Monitor snap operation tasks currently running or waiting to execute in the Task Monitoring panel. You can configure the length of the visible task queue by selecting the General Settings tab of the Administration window.

This task queue setting is also configurable in the `$SMU_HOME/etc/smu.conf` file by setting the parameter `task.queue.length`. The parameter's default is 100. Restart SMU in order for the parameter setting change to take effect.

Managing snap backup initiation in the Schedules tab

Figure 15 shows the BUI displayed by selecting the Schedules tab.

![Figure 15. Viewing a selected application's scheduled backups](image)

The displayed table shows a list of snap backup schedules for the selected application and includes the following items:

- Frequency – Hour, Day, Week, Month.
Day – Day of the week.
Hour – The hour the snap backup will be taken.
Minute – The minute the snap backup will be taken.
Retention – Number of snap backups that will be retained.
Backup Type – Offline or Online.
Description – Brief description of this entry entered by the user.

Adding a schedule
1. Click on Actions and Add.
2. Enter the values for Frequency, Day of Month, Day of Week, Hour, Minute, Retention, Backup Type and Description.
3. Click OK.

This entry will show up in the table under the Schedules tab for this application. The snap backups will be taken for this application according to the schedule just created.

Editing a schedule
1. Select an application of your choice and an entry from the table under the Schedules tab that you want to edit.
2. Click on Actions and Modify.
3. Edit the values for Frequency, Day of Month, Day of Week, Hour, Minute, Retention, Backup Type and Description.
4. Click OK.

The edited schedule will be reflected in the table under the "Schedules" tab for the selected Application.

IMPORTANT: If a backup schedule is modified while its auto backup is currently in process, this backup will not be managed by the new retention policy for the edited schedule. The backup should be manually deleted when the backup is no longer used.
Deleting a schedule
1. Select an application of your choice and an entry you want to delete from the table under the Schedules tab.
2. Click on Actions and Remove.
3. Click OK to confirm the delete operation. This will delete the selected schedule you created for taking snap backups for the selected application.

Monitoring snap operation tasks
The Task Monitoring Table lists tasks currently running, completed or waiting in the queue to be processed. The Task Monitoring Table displays ID, Application, Task (snap operation), Description, Start Time, End Time, and Status. The Application column displays the name of the snap operation target application in a hypertext link. Clicking on the application name, you can navigate to the Snap Backups Summary page of the application.

The Status column displays the status of the task with a status icon. Clicking on the status icon launches the task output window where you can view the detailed task output. By selecting a particular status icon among the set of status icons on the right upper corner of the Task Monitoring Table panel, you can list tasks only in that status.

Canceling currently running tasks
To cancel a currently running task, select the task and click on the cancel button. It is very important to be aware that canceling a task may leave the underlying application or resources in an inconsistent state. Therefore, cancel a task with caution.

Deleting task history
Delete any completed tasks of no further interest for review from the Task Monitoring Table by selecting the task and clicking on the delete button. If you need to track back to the deleted task, you can still view its task output on the Activity Logs page.

Managing account settings using the Account Settings tab
Figure 16 shows the basic account information displayed using the Account Settings tab for a selected application. In this tab, you can make basic modifications to the Application, Application Host, and Storage settings by selecting their corresponding right-sided change buttons and filling out the appropriate editable fields.
If a selected application account has backups under it, neither the Application Host nor Storage settings can be modified; the Change Host/Change Storage button will not display.

Figure 16. Displaying account configuration in the Account Settings tab

Managing Activity Logs Using the BUI

Located below the Accounts category in the left-side Workgroup area of the BUI, the Activity Logs category contains information on the past user-initiated activity that has taken place with the Snap Management Utility. The Activity Logs display parameters and navigation are highly customizable for the user.

The Actions and View bar also include the following separate action icons, whose functions can also be selected in either the Actions or View pull-down menus. Mousing over them displays their name/function:

- Filter Activity Logs – Filter by Log ID, User, Application, Action, Task or Status.
- Export Activity Logs – Specify beginning and ending log ID numbers for the range to export. The exported range of logs will appear in the Tasks window, and can be detached as a separate table display window for easier inspection as well as maintaining a record of them before purging logs.
- Purge Activity Logs – Delete a selected range, specified by beginning and ending log IDs, from the Activity Logs. As noted in Export Activity Logs, use that function to save a record of logs before purging them.

Clicking on “Activity Logs” generates a display with the following column items:
ID – The system-generated unique identification number for each of the activities.
User – The SMU user name for who initiated the particular activity.
Application – The name of the application for which the activity was initiated.
Action – The action that was initiated by the user.
Task – The numeric ID assigned for a task generated from a user-initiated action.
Description – A brief description of the activity.
Time – The time the activity was initiated.
Status – Indicates whether the activity was successfully completed or not.

These column displays can be individually hidden or selected for display using the View pull-down menu, Columns setting.

Figure 17 shows the BUI screen for Activity Logs.

![Figure 17. Displaying the activity logs in the SMU BUI](image)

When a user action is performed as a task, the activity log(s) for the user action will display a task ID in the Task field. The task ID is a hyperlink that links to the corresponding line in the Tasks panel below the Activity Logs window.

You can view completed task output by clicking the hyperlink in the Task field in the Activity Logs window or, by clicking the associated Output field icon for the task in the Tasks panel, you can view not only completed task output but also running task output in real-time.

On the right side of the display, scroll arrows for up, down, first, last, previous and next task items are selectable. The Jump To tab, when selected, presents a dialog box to choose a task ID for display. Figure 18 shows an example popup screen showing output for task ID 104.
A user action performed as a task will have two activity log entries: one for task submission and another for task completion (status could be succeeded, failed, canceled, for example). Neither intermediary (sub) actions or task deletions will record activity logs.

Filtering Activity Logs

The Activity Logs window contains configurable filters that, once selected, are persistent per that user’s setup. The optional fields for use as filters include: Log ID, User, Application, Action, Task, and Status.

The filters for Log ID and Task use the form of an ID range that can be expressed with a comparison operator followed by a number (ID). The supported comparison operators are listed in the following table.

If you are viewing the Activity Logs window and do not see the expected rows in the activity table, check to see if any filter criteria are specified. Change or reset the criteria to view the activity logs you are interested in.

<table>
<thead>
<tr>
<th>OPERATOR</th>
<th>SEARCH PARAMETER</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;n</td>
<td>Search for logs whose ID is greater than n</td>
<td>&gt;10 returns logs whose ID is greater than 10</td>
</tr>
<tr>
<td>&gt;=n</td>
<td>Search for logs whose ID is greater than or equal to n</td>
<td>&gt;=20 returns logs whose ID is greater than or equal to 20</td>
</tr>
<tr>
<td>=n</td>
<td>Search for logs whose ID equals n</td>
<td>=30 returns logs for ID number 30</td>
</tr>
<tr>
<td>&lt;=n</td>
<td>Search for logs whose ID is less than or equal to n</td>
<td>&lt;=40 returns logs whose ID is less than or equal to 40</td>
</tr>
</tbody>
</table>
TABLE 9. ACTIVITY LOG FILTER SPECIFICATIONS

<table>
<thead>
<tr>
<th>OPERATOR</th>
<th>SEARCH PARAMETER</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;n</td>
<td>Search for logs whose ID is less than n</td>
<td>&lt;50 returns logs whose ID is less than 50</td>
</tr>
<tr>
<td>n-nn</td>
<td>Search for logs whose ID is between n and nn</td>
<td>60-70 returns logs whose ID is between 60 and 70</td>
</tr>
</tbody>
</table>

The filter for the rest of the fields is the text search filter. This filter allows the wildcard character %. Example uses are:

- %xyz – Search for the text fields whose value ends with xyz.
- xyz% – Search for the text fields whose value starts with xyz.
- %xyz% – Search for the text fields whose value contains xyz.

When no wildcard characters are used, the filter finds the exact match. The text comparison of the text search filter is case sensitive.

By default, activity logs are fetched up to 10,000 entries. The max rows to fetch can also be configured using the actlog.max_fetch parameter of the smu.conf file. Note that this parameter setting will apply across the particular SMU application, so it will apply to all SMU users. If the smu.conf file has been changed, the Snap Management Utility must be stopped and restarted in order to activate the new smu.conf file parameter settings.

**Exporting Activity Logs**

To export a range of activity log entries:

1. Either select Actions and Export in the Actions pull-down menu, or select the Export Activity Log icon next to the Filter (funnel-shaped) icon.
2. Provide values for the task ID range you would like to export, in Begin ID and End ID.
3. Select OK.
4. The Export Activity Logs operation will appear in the Tasks window, as shown in the following figure. Click on the green Success checkmark icon in the Status column of the newly executed Export Activity Logs task to see the details of this operation, including the name of the zip file that the operation creates to hold the activity logs for the specified task IDs.
Purging Activity Logs

To purge a selected range of tasks in the Activity Logs window:

1. Either select the Purge Activity Logs icon (crossbar) or select Actions, Purge. A popup window provides a warning reminder that, upon the purge operation's completion, the selected task IDs will be permanently deleted and should first be backed up to a file using the Export operation.

2. Provide entries for the Begin ID and End ID task numbers which indicate the range of task IDs to purge.

3. Verify that you are committing to deletion of these entries by typing "Yes" in the Confirm box.

4. Select OK.

Using the Command-Line Interface

Once you have accessed the CLI you are presented with the SMU shell. The prompt `smu>` is displayed. You can type SMU commands at the SMU prompt. The following command categories are available:
<table>
<thead>
<tr>
<th>COMMAND CATEGORY</th>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts</td>
<td>accounts</td>
<td>Accounts used to access remote resources such as databases, database hosts, or RAC cluster nodes and Oracle ZFS Storage appliances.</td>
</tr>
<tr>
<td>Activities</td>
<td>activities</td>
<td>A record of all actions performed by SMU users that can be used for auditing purposes.</td>
</tr>
<tr>
<td>Alerts</td>
<td>alerts</td>
<td>Actions SMU will take when events such as task failures or task cancellations occur.</td>
</tr>
<tr>
<td>Backups</td>
<td>backups</td>
<td>Backups created by the user manually or automatically by a schedule.</td>
</tr>
<tr>
<td>Certificates</td>
<td>certs</td>
<td>Certificates used by the embedded SMU WinRS and web servers. For the v1.0 release, only the self-signed SSL certificate is managed.</td>
</tr>
<tr>
<td>Keys</td>
<td>keys</td>
<td>SSH public keys of SMU users. This allows you to log in to SMU using SSH with key-based authentication instead of password-based authentication.</td>
</tr>
<tr>
<td>Schedules</td>
<td>schedules</td>
<td>Schedule automatic backups with optional retention policies.</td>
</tr>
<tr>
<td>Tasks</td>
<td>tasks</td>
<td>Background tasks. SMU performs all snapshot-based operations as background tasks since they involve logging into and coordinating remote resources and executing a series of commands that can take a long time to complete.</td>
</tr>
<tr>
<td>Users</td>
<td>users</td>
<td>SMU users. Both local and directory users are supported.</td>
</tr>
</tbody>
</table>

Each command category supports a set of subcommands to manage the category objects. Most categories follow the add/modify/remove idiom, which allows you to, respectively, add new objects, modify existing objects and remove objects. All categories support the get and list methods. These methods are used to display the objects in property list or tabular format.

The following example shows the syntax of each subcommand supported in each command category.
To create a new object:

```
add [category options] [-o property=value] ... name
```

where:

- **category options** – Specifies one or more category options (depending on the command category). Additionally, you can specify general properties of the object.
- **-o property=value** – Sets the specified property. Multiple `-o` options can be specified.
- **name** – Creates the new object with the specified name.

To display properties for a given object:

```
get [-H] [-o all | field[, ...]] all | property[, ...] [name] ...
```

where:

- **-H** – Displays output in a form more easily parsed. Headers are omitted and fields/columns are separated by a single tab instead of an arbitrary amount of space.
- **-o field** – Sets the fields to display, which includes one or more of name, property, or value. Present multiple fields as a comma-separated list. The default value is: `name,property,value`. The special value `all` will display all properties.
- If no object names are specified, then the command displays properties for all objects in that command category. For each property, these columns are displayed:
  
  | name     | Object name or identifier |
  | property | Property name             |
  | value    | Property value            |

To list property information for the given datasets in table form:

```
list [-H] [-o property[, ...]] [ -s property ] ... [ -S property ] ... [name] ...
```

where:

- **-H** – Suppresses printing of headers. Fields are separated by a single tab instead of arbitrary white space.
• `-o property` – A comma-separated list of properties to display.

• `-s property` – A property for sorting the output by column in ascending order based on the value of the property. Multiple properties can be specified at one time using multiple `-s` property options. Multiple `-s` options are evaluated from left to right and establish the sorting precedence.

• `-S property` – Same as the `-s` option but sorts by property in descending order.

To modify one or more properties of an object:

```
modify [-o property=value] ... name
```

where:

• `-o property=value` – Sets the specified property. Multiple `-o` options can be specified.

• `name` – Name of the object whose property will be modified.

To remove an object:

```
remove [-F] name
```

where:

• `name` – Lists the object to be deleted from the command category.

• `-F` – Forcibly removes the object. Without this option, SMU will prompt the user to confirm before removing the object.

Managing Accounts

SMU accesses and coordinates various application and system resources while performing operations. In order to access these resources, the user must supply the accounts for SMU to use. Each account has a type and protocol. The type identifies what type of resource the account is for: application, host, or storage. The protocol identifies what method is used to access the resource. Each protocol has a set of properties that must be specified. Some properties have defaults; others require setting their values. The following table lists the accounts supported by SMU along with their type and properties:
### Table 11. Supported Accounts Accessed by Snap Management Utility

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Account Protocol (Oracle Database)</th>
<th>Properties (Default Value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>ORACLE_DATABASE</td>
<td>cluster_database (false)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>oracle_sid (orcl)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port (1521)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>storage</td>
</tr>
<tr>
<td>HOST</td>
<td>SSH2 (Secure Shell Version 2)</td>
<td>hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port (22)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user (root)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>delegate (none)</td>
</tr>
<tr>
<td>HOST</td>
<td>WINRS (Windows Remote Shell)</td>
<td>hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port (5986)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user (Administrator)</td>
</tr>
<tr>
<td>Storage</td>
<td>SUN_ZFS_STORAGE</td>
<td>hostname</td>
</tr>
<tr>
<td></td>
<td>(Oracle ZFS Storage Appliance)</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port (22)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user (root)</td>
</tr>
</tbody>
</table>

At a minimum, you must add one account of each type in order to perform any SMU tasks. Additionally, the application account must reference a host and storage account through the properties, which is how you associate or link the application to its hardware resources; namely, the host the application is running on and the storage the application is using.

The following table lists actions that can be performed on accounts. Command examples follow.
TABLE 12. PERMISSIBLE ACTIONS ON ACCOUNTS

<table>
<thead>
<tr>
<th>ACCOUNTS SUBCOMMANDS</th>
<th>DESCRIPTION</th>
<th>SYNPYISIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add an account</td>
<td>accounts add [-t type] [-p protocol] [-o option] ... name</td>
</tr>
<tr>
<td>get</td>
<td>Get account properties</td>
<td>accounts get [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list</td>
<td>List accounts</td>
<td>accounts list [-t type] [-a</td>
</tr>
<tr>
<td>modify</td>
<td>Modify an account</td>
<td>accounts modify [-o option] ... name</td>
</tr>
<tr>
<td>remove</td>
<td>Remove an account</td>
<td>accounts remove [-F] name</td>
</tr>
<tr>
<td>test</td>
<td>Test an account</td>
<td>accounts test name</td>
</tr>
</tbody>
</table>

To set or modify the account password property

Each account has a password property. This property value can be supplied on the SMU accounts command line or can be entered interactively with no character echoing. SMU will prompt for the password if it is not specified on the accounts command line in the following fashion when adding a new account:

Type password:
Re-type password:

To modify an account password interactively, clear the password on the accounts modify command line:

smu> accounts modify -o password= <account name>
Type password:
Re-type password:
smu>

To add an Oracle ZFS Storage Appliance account

smu> accounts add -t STORAGE -p SUN_ZFS_STORAGE -o hostname=<hostname> -o user=<user> -o port=<port> -o password=<password> <account name>
To add a UNIX host account

```
smu> accounts add -t HOST -p SSH2 -o hostname=<hostname> -o user=<user> -o port=<port> -o password=<password> -o delegate=<NONE/SUDO> <account name>
```

To add a Windows host account

```
smu> accounts add -t HOST -p WINRS -o hostname=<hostname> -o user=<user> -o port=<port> -o password=<password> <account name>
```

To add an Oracle Database account

```
smu> accounts add -t APPLICATION -p ORACLE_DATABASE -o cluster_database=<true|false> -o host=<host account> -o oracle_sid=<SID> -o password=<password> -o port=<port> -o storage=<storage account> <account name>
```

To get all of the properties of every account

```
smu> accounts get all
```

To list accounts

```
smu> accounts list
```

To list accounts of a specified type*

```
smu> accounts list -t type
```

* Values for type can be application, host, or storage (Both uppercase and lowercase letters are accepted for these entries.)

To list application accounts with their associated details*

```
smu> accounts list -a
```

*including their associated properties names, host and storage accounts, origin of the clone and clone method

To list clones of the specified applications

```
smu> accounts list -c [app]
```
To modify an account

```
smu> accounts modify -o property=value ... <account name>
```

To remove an account

```
smu> accounts remove <account name>
```

You cannot remove application accounts that have backups. All backups of the application must be deleted before you can remove the application account.

You cannot remove host accounts that are referenced from an application account. All application accounts that reference the host account must be removed first.

You cannot remove storage accounts that are referenced from an application account. All application accounts that reference the storage account must be removed first.

Managing Activities

SMU keeps a record of all commands run by the user through the CLI or BUI using an activity log. Each activity record has the following fields:

<table>
<thead>
<tr>
<th>ACTIVITIES FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Activity integer identifier</td>
</tr>
<tr>
<td>time</td>
<td>The time of the activity</td>
</tr>
<tr>
<td>user</td>
<td>The user performing the activity</td>
</tr>
<tr>
<td>action</td>
<td>The action performed by the user</td>
</tr>
</tbody>
</table>

The activity log will grow over time as the software is used. Trim the activity log by removing older records. The following table lists permitted actions that can be performed on activities.
### Table 14. Permitted Actions on Activities

<table>
<thead>
<tr>
<th>ACTIVITIES</th>
<th>DESCRIPTION</th>
<th>SYNOPSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Get activity properties.</td>
<td>activities get [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list</td>
<td>List activity.</td>
<td>activities list [-H] [-o property[,...]] [-s property] ... [-S property] ... [id] ...</td>
</tr>
<tr>
<td>purge</td>
<td>Purge activit(ies).</td>
<td>activities purge &lt;id1-id2</td>
</tr>
</tbody>
</table>

To get all of the properties of activities

```
smu> activities get all
```

To list activities

```
smu> activities list
```

To purge a range of activities

```
smu> activities purge <id1-id2>
```

### Managing Alerts

The software can be configured to alert the user when certain events occur. The following event alerts are supported:

#### Table 15. Configurable Event Alerts

<table>
<thead>
<tr>
<th>EVENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TASK</td>
<td>A task has been canceled.</td>
</tr>
<tr>
<td>CANCELLED</td>
<td></td>
</tr>
</tbody>
</table>
TASK FAILED  A task has failed.

The following actions can be performed when an event occurs:

**TABLE 16. PERMISSIBLE ACTIONS FOR EVENT OCCURRENCES**

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
<th>PROPERTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMAIL</td>
<td>Send an email message.</td>
<td>address, subject</td>
</tr>
</tbody>
</table>

The EMAIL action requires that a list of email addresses and a subject line be specified for the mail message. You can specify multiple recipients for the address property by listing multiple email addresses separated by a comma.

The following actions can be performed on alerts.

**TABLE 17. PERMISSIBLE ALERT ACTIONS**

<table>
<thead>
<tr>
<th>ACCOUNTS SUBCOMMANDS</th>
<th>DESCRIPTION</th>
<th>SYNOPSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add an alert.</td>
<td>alerts add [-o option] ... event action</td>
</tr>
<tr>
<td>get</td>
<td>Get alert properties.</td>
<td>alerts get [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list</td>
<td>List alerts.</td>
<td>alerts list [-H] [-o property[,...]] [-s property] ... [-S property] ... [event:action] ...</td>
</tr>
<tr>
<td>modify</td>
<td>Modify an alert.</td>
<td>alerts modify [-o option] ... event action</td>
</tr>
<tr>
<td>remove</td>
<td>Remove an alert.</td>
<td>alerts remove [-F] event action</td>
</tr>
</tbody>
</table>

To send an email alert when a task fails

```
smu> alerts add -o address=<address-list> -o "subject=<subject>" TASK_FAILED EMAIL
```
To get all of the properties of every alert

```
smu> accounts get all
```

To list alerts

```
smu> alerts list
```

To modify an alert

```
smu> alerts modify -o property=value ... <event> <action>
```

To remove an alert

```
smu> alerts remove <event> <action>
```

Managing Backups

The software allows you to create on-disk backups of databases that use the Oracle ZFS Storage Appliance for storage. These backups are based on creating ZFS snapshots of the database shares, so they are only suitable for a specific class of use cases in which the user wants to make a quick backup for development or testing purposes. The backups can be used to restore or clone the database. Backups are added and removed by running the appropriate task (see Managing Tasks for more information).

The following actions can be performed on backups:

**TABLE 18. PERMISSIBLE BACKUP MANAGEMENT ACTIONS**

<table>
<thead>
<tr>
<th>BACKUPS MANAGEMENT SUBCOMMANDS</th>
<th>DESCRIPTION</th>
<th>SYNOPSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>get</td>
<td>Get backup properties.</td>
<td>backups get [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list</td>
<td>List backups.</td>
<td>backups list [-H] [-o property[,...]] [-s property] ... [-S property] ... [-t app[,...]] [app:name] ...</td>
</tr>
<tr>
<td>modify</td>
<td>Modify a backup.</td>
<td>backups modify [-o option] ... app:name</td>
</tr>
</tbody>
</table>
To get all of the properties of every backup
   smu> backups get all

To list backups
   smu> backups list

To modify a backup
   smu> backups modify -o property=value ... <app> <name>

Managing Certificates

The software uses a single self-signed certificate for encrypting Windows Remote Shell (WinRS) client and web browser sessions. The certificate is generated the first time SMU is started and is saved to a keystore file for subsequent use.

The following actions can be performed on certificates.

### TABLE 19. PERMISSIBLE CERTIFICATE ACTIONS

<table>
<thead>
<tr>
<th>CER TS</th>
<th>DESCRIPTION</th>
<th>SYNP OSI S</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUBCOM MANDS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>get get certificate properties.</td>
<td></td>
<td>certs get [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list List certificates.</td>
<td></td>
<td>certs list [-H] [-o property[, ...]] [-s property] ... [-S property] ... [alias] ...</td>
</tr>
</tbody>
</table>

To get all of the properties of every certificate
   smu> certs get all

To list certificates
   smu> certs list
Managing Keys

The software allows you to administer SSH2 public keys that can be used to perform key-based authentication in place of password-based authentication when connecting to SMU using an SSH client. A key has the following properties:

**TABLE 20. KEY PROPERTIES**

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>An alias for the key.</td>
</tr>
<tr>
<td>encoded</td>
<td>The SSH public key encoded in ssh-dss or ssh-rsa format. See <a href="http://www.ietf.org/rfc/rfc4253.txt">http://www.ietf.org/rfc/rfc4253.txt</a> for more information.</td>
</tr>
</tbody>
</table>

The following actions can be performed on keys.

**TABLE 21. PERMISSIBLE KEYS ACTIONS**

<table>
<thead>
<tr>
<th>KEYS SUBCOMMANDS</th>
<th>DESCRIPTION</th>
<th>SYNOPSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add a key.</td>
<td>keys add alias encoded</td>
</tr>
<tr>
<td>get</td>
<td>Get key properties.</td>
<td>keys get [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list</td>
<td>List keys.</td>
<td>keys list [-H] [-o property[,,...]] [-s property] ... [-S property] ...</td>
</tr>
<tr>
<td>remove</td>
<td>Remove a key.</td>
<td>keys remove [-F]</td>
</tr>
</tbody>
</table>

To add an ssh-dss key with the alias mykey

```
smu> keys add mykey
AAAAAB3NzaC1kc3MAAACABAJM3cknqShlHI8E9EXWXYgM/XeL1+0jccFG3C/W7C7dD6dLx1AOW5Tv671e/ils1N9be8KEI2DxS5/wnRkyRomhjHMs7TEYDzHRoWS5gzM393pkkNiwdo02B9fUo2Rpa1imBHQ+G09FQC0LP1SKfYClup0UIKg8H3XDCSuttGBAAAFQDwhT/KGyLRCpaYNbieuzfYcOywAKAIBEC/PeEe2k8Gt8IgiYsZj7tw/aHocu4/Kri2cqoCDTKHKW081E+ZHq0tUR6vfoOfdthsCX3Qiqh3ufYItR0BR5qTS5AW5cESnIN/orWCxvbRkuLOxtAaq1GjZaV+cGLmJvWaRtIYhB68j7NxbsUoyW9ryRbt0TQCv++/JrLGW/GAAAAIEAi0u0+lFkWNapbsf09TbBwaoA2avj8ciz7KUFyXmu99fjKOAVL0K4uVNnsnwy4g1MGVmxEQQVxcmZ2h/WPf1tvRKr2n5TmlAIdtJkIr3FOJ7XXszCt7Mq6JHEy/oRqJWnkETYhp8LOGigZBh9mfU4B5id+TZQRtqmz2qRU82H6JEg=
```
To get all of the properties of every key
smu> keys get all

To list keys
smu> keys list

To remove a key
smu> keys remove <alias>

Managing Schedules

The software allows you to schedule automatic backups at regular intervals such as hourly, daily, weekly or monthly. Additionally, each schedule can retain a set number of backups. For example, you can schedule automatic backups to occur daily and retain the seven (7) most recent backups.

The following schedule frequencies are available along with the day, hour and minute ranges.

<table>
<thead>
<tr>
<th>SCHEDULE FREQUENCIES</th>
<th>DAY RANGE</th>
<th>HOUR RANGE</th>
<th>MINUTE RANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>hour</td>
<td>-1</td>
<td>-1</td>
<td>0-59</td>
</tr>
<tr>
<td>day</td>
<td>-1</td>
<td>0-23 (0 = midnight)</td>
<td>0-59</td>
</tr>
<tr>
<td>week</td>
<td>1-7 (day of the week, 1=Sun, 7=Sat)</td>
<td>0-23 (0 = midnight)</td>
<td>0-59</td>
</tr>
<tr>
<td>month</td>
<td>1-31 (day of the month)</td>
<td>0-23 (0 = midnight)</td>
<td>0-59</td>
</tr>
</tbody>
</table>

The following actions can be performed on schedules.
## TABLE 23. PERMISSIBLE ACTIONS AND RELATED SUBCOMMANDS FOR SCHEDULES

<table>
<thead>
<tr>
<th>SCHEDULES SUBCOMMANDS</th>
<th>DESCRIPTION</th>
<th>SYNOPIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add a schedule.</td>
<td>schedules add [-k keep] [-d desc] [-o option] ... app freq day hour minute</td>
</tr>
<tr>
<td>get</td>
<td>Get schedule properties.</td>
<td>schedules get [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list</td>
<td>List schedules.</td>
<td>schedules list [-H] [-o property[, ...]] [-s property] ... [-$ property] ... [app:freq:day:hour:minute] ...</td>
</tr>
<tr>
<td>modify</td>
<td>Modify a schedule.</td>
<td>schedules modify [-k keep] [-d desc] [-o option] ... app freq day hour minute</td>
</tr>
<tr>
<td>remove</td>
<td>Remove a schedule.</td>
<td>schedules remove [-F] app freq day hour minute</td>
</tr>
<tr>
<td>rename</td>
<td>Modify frequency, day, hour, minute of a schedule</td>
<td>schedules rename app:freq:day:hour:minute freq day hour minute</td>
</tr>
</tbody>
</table>

To schedule an online backup at the top of every hour
```
smu> schedules add -o type=online <app> hour -1 -1 0
```

To schedule an offline backup at midnight every day
```
smu> schedules add -o type=offline <app> day -1 0 0
```

To schedule a backup every Friday at 5:00 p.m.
```
smu> schedules add <app> week 6 17 0
```

To schedule a backup on the 15th day of every month at 4:30 a.m.
```
smu> schedules add <app> month 15 4 30
```
To get all of the properties of every schedule

```
smu> schedules get all
```

To list schedules

```
smu> schedules list
```

To modify a schedule

```
smu> schedules modify [-k keep] [-d desc] -o property=value ... <app> <freq> <day> <hour> <minute>
```

To modify frequency, day, hour, minute of a schedule to the 15th day of every month at 4:30 a.m

```
smu> schedules rename <app>:<freq>:<day>:<hour>:<minute> month 15 4 30
```

**IMPORTANT:** If a backup schedule is modified while its auto backup is currently in process, this backup will not be managed by the new retention policy for the edited schedule. The backup should be manually deleted when the backup is no longer used.

To remove a schedule

```
smu> schedules remove [-F] <app> <freq> <day> <hour>
```

---

**Managing Tasks**

The software uses tasks to carry out database backup and recovery operations in addition to database cloning. Tasks are designed to run in the background and can take a long time to finish. The task manager is used to submit and run tasks. The following commands can be run as tasks.

**TABLE 24. PERMISSIBLE TASK COMMANDS**

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
<th>SYNOPSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>Back up a database (create a snap backup).</td>
<td>backup [-o type=ONLINE</td>
</tr>
</tbody>
</table>
clone       Clone a database from a snap backup.       clone [-o option]<source app> <source backup> <target app>

deprovision  Deprovision (delete) a clone database.        deprovision <app>
delete       Delete a snap backup.                      delete <app> <backup name>

import       Clone a database from an RMAN image copy backup. import <mountpoint> <app>

rename       Rename an existing backup.                  rename <app> <old backup name> <new backup name>

restore      Restore from a snap backup.                 restore [-F] <app> <backup name>

The following table provides further details for command options.

**TABLE 25. AVAILABLE TASK COMMAND OPTIONS**

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>type</td>
<td>The type of snap backup to create. Either OFFLINE or ONLINE. OFFLINE is the default when this option is not specified.</td>
</tr>
<tr>
<td>clone</td>
<td>type</td>
<td>The type of clone to create. Currently, the only supported type is PRIMARY, which means create a new primary database.</td>
</tr>
<tr>
<td>clone</td>
<td>oracle_home</td>
<td>The Oracle Home, or Oracle home directory, the clone database should use. The default is to use the same Oracle Home of the database whose backup is being cloned. The Oracle Home (database version) of a clone operation's target can only vary from the original Oracle Home by the version's fifth digit.</td>
</tr>
<tr>
<td>clone</td>
<td>db_name</td>
<td>The database name the clone database should use. The default is to set the database name to the oracle_sid of the clone database account.</td>
</tr>
</tbody>
</table>
TABLE 25. AVAILABLE TASK COMMAND OPTIONS

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>import</td>
<td>oracle_home</td>
<td>The Oracle Home the clone database should use. There is no default. This option must be specified. The Oracle Home (database version) of a clone operation's target can only vary from the original Oracle Home by the version's fifth digit.</td>
</tr>
<tr>
<td>import</td>
<td>db_name</td>
<td>The database name the clone database should use. There is no default. This option must be specified.</td>
</tr>
</tbody>
</table>

The following actions can be performed on tasks.

TABLE 26. PERMISSIBLE TASK ACTIONS

<table>
<thead>
<tr>
<th>TASKS SUBCOMMANDS</th>
<th>DESCRIPTION</th>
<th>SYNOPSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add a task.</td>
<td>tasks add [-f] [-F] command [options] arguments</td>
</tr>
<tr>
<td>cancel</td>
<td>Cancel a task.</td>
<td>tasks cancel [-F] id</td>
</tr>
<tr>
<td>cat</td>
<td>Display task output.</td>
<td>tasks cat id</td>
</tr>
<tr>
<td>get</td>
<td>Get task properties.</td>
<td>tasks [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list</td>
<td>List tasks.</td>
<td>tasks list [-H] [-o property[,....]] [-s property] ... [-S property] ...</td>
</tr>
<tr>
<td>remove</td>
<td>Remove a task (must have finished running).</td>
<td>tasks remove [-F] id</td>
</tr>
<tr>
<td>tail</td>
<td>Tail task output (watch output as it is written).</td>
<td>tasks tail [-c chars][-f] [-n lines] id</td>
</tr>
<tr>
<td>wc</td>
<td>Display task output size in characters and lines.</td>
<td>tasks wc [-c] [-l] id</td>
</tr>
</tbody>
</table>
To add a default (offline) backup task

```
smu> tasks add backup <app> <backup name>
```

To add an online backup task

```
smu> tasks add backup -o type=ONLINE <app> <backup name>
```

To add a restore task

```
smu> tasks add restore <app> <backup name>
```

To add a clone task where the snap backup `<backup>` of app `<app1>` is cloned to app `<app2>`

```
smu> tasks add clone <app1> <backup> <app2>
```

To add a clone task where the snap backup `<backup>` of app `<app1>` is thin cloned to app `<app2>`

```
smu> tasks add clone <app1> <backup> <app2>
```

To add a clone task where the snap backup `<backup>` of app `<app1>` is split cloned to app `<app2>`

```
smu> tasks add clone <app1> <backup> <app2>
```

To add a clone task where the snap backup `<backup>` of app `<app1>` is split cloned to app `<app2>` and the clone is provisioned as a standby database.

```
smu> tasks add clone <app1> <backup> <app2>
```

To add a clone task where the snap backup `<backup>` of app `<app1>` is split cloned to app `<app2>` and the clone is provisioned as a standby database.

```
smu> tasks add clone <app1> <backup> <app2>
```

To add an import task where the RMAN backup in share `<mountpoint>` is cloned to app `<app>`

```
smu> tasks add import <mountpoint> <app> -o oracle_home=<oracle-home> <backup-shares-mountpoint-list> <app>
```

Where `<oracle-home>` is the Oracle home to use for the clone database (and must be specified), `<backup-shares-mountpoint-list>` is a comma-separated list of the backup share mountpoints to create the clone from, and `<app>` is the database account to use for the clone database.
The mountpoint list can specify share mountpoints from either head/controller of a clustered Oracle ZFS Storage Appliance. The backup can span both heads of a clustered Oracle ZFS Storage Appliance. For more descriptions of the mountpoint property, refer to the List of Shares table in the Oracle ZFS Storage Appliance on-line help, section Shares:Shares.

To get all of the properties of tasks
```
smu> tasks get all
```

To list tasks
```
smu> tasks list
```

To list tasks of a specific type
```
smu> tasks list -t <type[,...]>
```
where the value for type can be backup, restore, clone, import, delete, deprovision, rename, export-log (case insensitive)

To list tasks of specific state(s)
```
smu> tasks list -T <state[,...]>
```
where the value for state can be SUBMITTED, PENDING, RUNNING, CANCELLED, FAILED, SUCCEEDED (case insensitive)

To display task <id> output
```
smu> tasks cat <id>
```

To watch task <id> output
```
smu> tasks tail -f <id>
```

To remove a completed task
```
smu> tasks remove <id>
```

You cannot remove tasks that have not finished running. You must either wait until the task completes or cancel the task before execution.
Managing Users

In order to access the user interfaces, you must first log in to your user account. These user accounts represent the list of users who can use the software. The software supports two types of users: local and LDAP. Local users are only defined within the context of the software. LDAP users are defined within the enterprise.

The following actions can be performed on users.

**TABLE 27. PERMISSIBLE ACCOUNT ACTIONS**

<table>
<thead>
<tr>
<th>USERS SUBCOMMANDS</th>
<th>DESCRIPTION</th>
<th>SYNOPSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add a user.</td>
<td>users add [-t type] [-o option] ... name</td>
</tr>
<tr>
<td>get</td>
<td>Get user properties.</td>
<td>users get [-H] [-o &quot;all&quot;</td>
</tr>
<tr>
<td>list</td>
<td>List users.</td>
<td>users list [-H] [-o property[,,...]] [-s property] ... [-S property] ... [name] ...</td>
</tr>
<tr>
<td>modify</td>
<td>Modify a user.</td>
<td>users modify [-o option] ... name</td>
</tr>
<tr>
<td>remove</td>
<td>Remove a user.</td>
<td>users remove [-F] name</td>
</tr>
</tbody>
</table>

To set or modify the user password property

Local users have a password property. Supply this property value either on the SMU user’s command line or enter it interactively with no character echoing. When adding a new account, SMU will prompt for the password if it is not specified on the user's command line:

Type password:
Re-type password:

To modify a user password interactively, clear the password on the `users modify` command line:

```
smu> users modify -o password= <account name>
Type password:
Re-type password:
```
smu>

To add a local user
smu> users add -t LOCAL -o gecos=<user fullname> -o password=<password> <name>

To get all of the properties of users
smu> accounts get all

To list users
smu> accounts list

To modify a user
smu> users modify -o property=value ... <user name>

To remove a user
smu> users remove <user name>

You cannot remove the admin user.
Troubleshooting – General Information

If encountering difficulties with operations in the Snap Management Utility, first verify that none of the restrictions listed in the quick reference table that follows have been overlooked.

For a list of known issues and required actions, go to My Oracle Support (MOS) at http://support.oracle.com. Do a search for Doc ID 1522925.1. Some of the more common issues have been contained in this document in a Troubleshooting Common Issues table that follows in Appendix E.

To report an issue that is still not resolvable, submit a service request (SR) to http://support.oracle.com. Please provide the following information along with your SR.

If the issue occurred using the CLI:

• Provide the command line output and all error messages output by the command.
• If the issue is due to a task failure, provide the task information and output.

If the issue occurred using the BUI:

• Indicate which user interface pane was being used, which table was displayed, and what table action was attempted.
• Describe any error dialog that appeared and what information was contained in it.
• If the issue is due to a task failure, provide the task information and output.

Additionally provide the following files from the software data directory:

• For Oracle Linux – /var/opt/oracle/smu
• For Oracle Solaris – /var/opt/ORCLsmu
• For Windows – C:\ProgramData\Oracle\Oracle Snap Management Utility
• smu.log.N
• SmuService.log.N (only present on Windows hosts)

SMU Restrictions Quick Reference Table

The following table provides a quick reference reminder of the restrictions that are applicable to each SMU operation. Failing to understand and follow any of these restrictions can cause the related operation to fail.
<table>
<thead>
<tr>
<th>OPERATION</th>
<th>RESTRICTIONS</th>
</tr>
</thead>
</table>
| Snap backup               | • Offline or online backups only.  
• Database shares must reside within a single pool.  
• Offline backups allow one or more shares with database files spread across them in any fashion.  
• Online backups require datafiles and archived logs be in separate shares; during an online backup the datafile shares are snapped first, the online logs are then archived, and finally the archived log shares are snapped.  
• Online backups are only supported with filesystem (NFS or dNFS) storage type.  
• ASM database only supports offline backup; it is not possible to separately snap datafiles and archived log files that are in a diskgroup.  
• When creating an offline backup of a clustered database, any database nodes that have been stopped but not disabled will be restarted at the end of the backup task when the software restarts the database. |
| Snap restore              | • Can only restore to backup if newer backups do not have any clones.  
• A restore to offline snap backup restores the database to a point in time when the database was shut down and snap backups were taken.  
• A restore to online snap backup restores the database by performing incomplete recovery to the point in time when the snap backup was taken; recovery is up through the point at which the database was taken out of backup mode. A new control file is created when the database is restored and an open resetlogs is performed. |
| Snap clone from snap backup | • Clones are exact copies of the origin/source; use the same memory model and memory sizes.  
• Clone shares are placed in the same project as original shares.  
• Clone LUNs are placed in the same initiator and target groups as the origin shares.  
• The target database's host oracle user must have the same uid and gid as the source database's host Oracle user.  
• The clone will use the same memory model as the original database.  
• If dNFS is desired for the clone database, it must be configured in the target Oracle home before the clone operation is performed. |
OPERATION RESTRICTIONS

<table>
<thead>
<tr>
<th>OPERATION</th>
<th>RULES</th>
</tr>
</thead>
</table>
| Snap clone from RMAN backup | • The backup must be in image copy format.  
• Only filesystem (NFS, dNFS) storage type clones are supported.  
• The backup must contain appropriate files (controlfile, datafiles and archivelogs). Files must be in %U format.  
• Only cloning from hot (online) backup is supported.  
• The controlfile must have appropriate rows in the v$datfile_copy about each datfile (change_check# must be correct).  
• Clone shares are placed in the same project as the backup shares.  
• The target database host must have the same version of Oracle software as the source database host; no upgrades are performed.  
• The target database’s host oracle user must have the same uid as the source database’s host oracle user.  
• No listener, tnsname or enterprise manager are configured for the clone.  
• You must specify Oracle home for clone database to use (a path like /u01/app/oracle/product/11.2.0/dbhome_1). The Oracle home must not end with a "/" (a slash character).  
• SMU must be able to mount a copy of the backup controlfile in order to query key system views for information about the backup. This requires starting up a temporary instance that uses the original database name, so there cannot be another database mounted on the target database host that uses the same name.  
• The clone will use the default settings for the memory-related parameters (ASMM memory model and 2GB SGA size).  
• The selected share(s) must contain a single RMAN backup set to be used in the clone operation. No other RMAN files or Oracle files may reside on the share(s).  
• The target host(s) must have data path connectivity to the Oracle ZFS Storage/Backup Appliance. |
### OPERATION RESTRICTIONS

<table>
<thead>
<tr>
<th>OPERATION</th>
<th>RESTRICTIONS</th>
</tr>
</thead>
</table>
| Deprovision snap clone | • The target database host must have the same version of Oracle software as the source database host; no upgrades are performed.  
• The database compatibility of the clone sets to the version of Oracle software installed on the target database host.  
• The database must be in the mounted state so that SMU can obtain the required information on it.  
• No listener, tnsname or enterprise manager are configured for the clone. |
Appendix A: References

- **Oracle ZFS Storage Appliance Administration Guide**

- Oracle Snap Management Utility for Oracle Database full documentation set
  [http://docs.oracle.com/cd/E39520_01/index.html](http://docs.oracle.com/cd/E39520_01/index.html)

- My Oracle Support (MOS)
  [http://support.oracle.com](http://support.oracle.com)

- Notes on RMAN Cloning, search for Doc ID 1210656.1
  My Oracle Support (MOS)
  [http://support.oracle.com](http://support.oracle.com)

- **Oracle® Database Platform Guide**
  11g Release 2 (11.2) for Microsoft Windows
  [http://docs.oracle.com/cd/E11882_01/win.112/e10845/architec.htm](http://docs.oracle.com/cd/E11882_01/win.112/e10845/architec.htm)

- **Oracle® Database Installation Guide**
  11g Release 2 (11.2) for Linux
  [http://docs.oracle.com/cd/E11882_01/install.112/e24321/toc.htm](http://docs.oracle.com/cd/E11882_01/install.112/e24321/toc.htm)

- *Creating Files on a NAS Device for Use with Oracle Automatic Storage Management*

- Sudo authorization delegation tool information and download
  [http://www.sudo.ws](http://www.sudo.ws)
  Oracle Solaris 10-compatible Sudo tool available on Oracle Solaris Companion CD
  [http://www.sunfreeware.com](http://www.sunfreeware.com)
Appendix B: Glossary

ASM | Automatic Storage Management. A type of filesystem that organizes database files into disk groups for ease of management, as ASM automates and manages the underlying database files.

Clone | A clone is an instantaneously created, read-writable copy of a snap backup. One or more clones can be created from a single snap backup. Clones are presented to users as a normal filesystem. The usual operations can be performed on clones. Clones are typically used in a test, development, QA, or backup environment.

Cluster | Multiple interconnected computers or servers that appear as if they are one server to end users and applications.

Cold backup | See proper term, offline backup.

Deprovision | The process of changing the state of a storage asset (share) as a usable resource for an application to unavailable.

dNFS | direct Network File System. An NFS client that optimizes I/O on Network Attached Storage (NA) devices.

FRA | Flash Recovery Area. A configured area of disk storage where backup components such as datafile image copies, archive logs, and controlfiles are held.

Hot backup | See proper term, online backup.

iSCSI | Internet Small Computer System Interface. A protocol that allows data packets to be transmitted using TCP/IP.

NFS | Network File System. A filesystem protocol used in Network Attached Storage (NAS) systems that allows the sharing of files, based on access privileges, among remote clients and the primary server.

Offline backup | Offline (also called cold) backups are backups taken when the database is shut down. The software will shut down the database temporarily and then restart it after taking the snap backups.

Online backup | Also referred to as hot backup. Online backups are taken when the database is placed into backup mode while remaining online. Online backups take snap backups of the database shares in a particular order and in between changing the database mode and archiving the current logs.

Project | An Oracle ZFS Storage Appliance project defines a common administrative control point for managing shares. All shares within a project can share common settings, and quotas can be enforced at the project level in addition to the share level. Projects are also used to group logically related shares together so their common attributes can be accessed from a single point. All filesystems and LUNs are grouped into projects. Typically, every application has its own project.

RAC | Oracle Real Application Clusters. A tool enabling the clustering of Oracle databases.

RMAN | A feature of the Oracle Database, Oracle Recovery Manager is a comprehensive tool for easily managing backup and recovery of Oracle Database and provides a common interface, either through a command line or Enterprise Manager, for backup tasks across different host operating systems.

Shares | Shares are filesystems and LUNs exported over supported data protocols to clients of the Oracle ZFS Storage Appliance. A share is created under a project. Filesystems export a file-based hierarchy and can be accessed over CIFS, NFS, HTTP/WebDAV and FTP. LUNs export block-based volumes and can be accessed through iSCSI.

SID | The Oracle System ID that uniquely identifies a particular database on a system. The variable for the
identifier is `ORACLE_SID`.

**Snap backup**

A snap backup is a read-only, point-in-time copy of a filesystem, instantaneously created with no space allocated initially. Blocks are allocated as changes are made to the base filesystem (copy on write). Snap backup data can be directly accessed for backup purposes, Snap backups are initiated either manually or through automated scheduling at specified intervals. Any reads to the snap backup blocks are served by the base filesystem’s block. As the changes occur to the base filesystem, the older block referenced by the snap backup and the new, changed block are referenced by the filesystem.

A project-level snap backup is the same as taking snap backups on all the shares within the project.

**Storage pool**

A storage pool is created among a set of physical disks. Filesystems are then created over the storage pool. One or more storage pools are created over the available physical disks.

**Sudo**

A privilege authorization program that allows a substitute user ("su") to execute programs ("do") using another user's security privileges, often the root user. The substitute user establishes a password connected to the desired privileged access that sudo verifies from its configuration file, then grants the requested access. Sudo was developed for Unix-like operating systems.

**Thin clone**

A clone of a snap backup which is created using Oracle ZFS Storage Appliance clone technology. A thin clone is created on the same storage pool as the source snap backup (called a clone point) and shares base data blocks with the base share and the source snap backup. As such, a thin clone has data dependencies to the source snap backup and the base share. Neither the base share or the source snap backup can be deleted unless the thin clone is removed.

**Wallet file**

An Oracle wallet file stores the master encryption key to an Oracle Database protected using transparent data encryption, which encrypts sensitive table data in the datafiles. Without access to the Oracle wallet, which is stored outside of the database, the database table data cannot be read and/or copied.
Appendix C: Icon Set for the SMU Browser User Interface

The following table lists all the icons used in the Browser User Interface and their associated meanings. Mousing over any of these icons produces a display of that icon's function.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action or entity it represents</th>
<th>Further information</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add action" /></td>
<td>Add action</td>
<td>Operation for Add Application, Add Backup, Add Schedule, Add Storage, Add Host, Add Notification, Add User.</td>
</tr>
<tr>
<td><img src="image" alt="Administrator image icon" /></td>
<td>Administrator image icon</td>
<td>Administration node in the navigation tree.</td>
</tr>
<tr>
<td><img src="image" alt="Clone creation icon" /></td>
<td>Clone creation icon</td>
<td>Operation for Create Primary clone.</td>
</tr>
<tr>
<td><img src="image" alt="Database Application image icon" /></td>
<td>Database Application image icon</td>
<td>Application node in the navigation tree.</td>
</tr>
<tr>
<td><img src="image" alt="Delete action" /></td>
<td>Delete action</td>
<td>Operation for Remove Application, Delete task from Tasks queue, Delete Backup, Remove Schedule, Remove Host, Remove Storage, Remove user, Remove Notification.</td>
</tr>
<tr>
<td><img src="image" alt="Edit/update action" /></td>
<td>Edit/update action</td>
<td>Operation for Modify Application, Rename Backup, Modify Schedule, Modify Host, Modify Storage, Modify user, Modify Notification.</td>
</tr>
<tr>
<td><img src="image" alt="Application root image icon" /></td>
<td>Application root image icon</td>
<td>Image icon of the applications root node in the navigation tree.</td>
</tr>
<tr>
<td><img src="image" alt="Export action" /></td>
<td>Export action</td>
<td>Operation for Export Activity Logs in the activity logs panel.</td>
</tr>
<tr>
<td><img src="image" alt="File import action" /></td>
<td>File import action</td>
<td>Operation for Import RMAN Backup Image in Applications panel.</td>
</tr>
<tr>
<td><img src="image" alt="Filter action" /></td>
<td>Filter action</td>
<td>Operation for Filter Activity Logs in Activity Logs panel.</td>
</tr>
<tr>
<td><img src="image" alt="User image icon" /></td>
<td>User image icon</td>
<td>Login User image icon in upper right header area of the main page.</td>
</tr>
<tr>
<td><img src="image" alt="Help for a topic" /></td>
<td>Help for a topic</td>
<td>Topic helper next to each field in a entry form panel.</td>
</tr>
<tr>
<td>Icon</td>
<td>Action or entity it represents</td>
<td>Further information</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><img src="image" alt="Running Tasks display option" /></td>
<td>Running Tasks display option</td>
<td>One of the options in upper right of Task panel for all the Running Tasks display. Also used as a task status indicator in the task table.</td>
</tr>
<tr>
<td><img src="image" alt="Activity Logs image icon" /></td>
<td>Activity Logs image icon</td>
<td>Activity Logs node image icon in the navigation tree.</td>
</tr>
<tr>
<td><img src="image" alt="Canceled Tasks display option" /></td>
<td>Canceled Tasks display option</td>
<td>One of the options in upper right of Task panel for the Canceled Tasks display. Also used as a task status indicator in the task table.</td>
</tr>
<tr>
<td><img src="image" alt="Failed Tasks display option" /></td>
<td>Failed Tasks display option</td>
<td>One of the options in upper right of Task panel for all the Failed Tasks display. Also used as a task status indicator in the task table.</td>
</tr>
<tr>
<td><img src="image" alt="Pending Tasks display option" /></td>
<td>Pending Tasks display option</td>
<td>One of the options in upper right of Task panel for all the Pending Tasks display. Also used as a task status indicator in the task table.</td>
</tr>
<tr>
<td><img src="image" alt="Succeeded Tasks display option" /></td>
<td>Succeeded Tasks display option</td>
<td>One of the options in upper right of Task panel for all the successful Tasks display. Also used as a task status indicator in the task table.</td>
</tr>
<tr>
<td><img src="image" alt="Restore Backup action" /></td>
<td>Restore Backup action</td>
<td>Operation for Restore Backup in the Application panel.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh panel/table action" /></td>
<td>Refresh panel/table action</td>
<td>Operation for Refresh Applications Table, Refresh Backups Table, Refresh Tasks Table.</td>
</tr>
<tr>
<td><img src="image" alt="Deprovision Application action; Purge Activity Logs action" /></td>
<td>Deprovision Application action; Purge Activity Logs action</td>
<td>Operation for Deprovision Application in Applications panel and Purge Activity Logs in Activity Logs panel.</td>
</tr>
<tr>
<td><img src="image" alt="Shuttle down (disabled is gray); shuttle down (enabled is blue)" /></td>
<td>Shuttle down (disabled is gray); shuttle down (enabled is blue)</td>
<td>Shuttle down operation for page navigation in Activity Logs panel and Backups panel.</td>
</tr>
<tr>
<td><img src="image" alt="Shuttle to the leftmost position (disabled: gray); (enabled: blue)" /></td>
<td>Shuttle to the leftmost position (disabled: gray); (enabled: blue)</td>
<td>Shuttle to the leftmost position operation for page navigation in Activity Logs panel and Backups panel.</td>
</tr>
<tr>
<td><img src="image" alt="Shuttle right (disabled: gray); (enabled: blue)" /></td>
<td>Shuttle right (disabled: gray); (enabled: blue)</td>
<td>Shuttle right operation for page navigation in Activity Logs panel and Backups panel.</td>
</tr>
<tr>
<td>Icon</td>
<td>Action or entity it represents</td>
<td>Further information</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>![ Shuttle to the rightmost position](disabled: gray); (enabled: blue)</td>
<td>Shuttle to the rightmost position operation for page navigation in Activity Logs panel and Backups panel.</td>
<td></td>
</tr>
<tr>
<td>![ Shuttle up](disabled is gray); shuttle up (enabled is blue)</td>
<td>Shuttle up operation for page navigation in Activity Logs panel and Backups panel.</td>
<td></td>
</tr>
<tr>
<td>![ Shuttle left](enabled: blue); (disabled: gray)</td>
<td>Shuttle left operation for page navigation in Activity Logs panel and Backups panel.</td>
<td></td>
</tr>
<tr>
<td><img src="red" alt=" Cancel Task action" /></td>
<td>Operation for Cancel Task in Tasks table.</td>
<td></td>
</tr>
<tr>
<td><img src="blue" alt=" All Tasks display option" /></td>
<td>One of the options in the upper right of Task panel for All Tasks display.</td>
<td></td>
</tr>
<tr>
<td><img src="green" alt=" Test Application action" /></td>
<td>Operation for Test Application to test for valid, accessible database.</td>
<td></td>
</tr>
<tr>
<td><img src="gray" alt=" Thin clone image icon" /></td>
<td>Thin clone node image icon in the navigation tree</td>
<td></td>
</tr>
</tbody>
</table>
Appendix D: Cloning Wallet Files for an Encrypted Database

When an Oracle Database is encrypted using the transparent data encryption feature, a random key that serves as the master encryption key is generated and stored in an Oracle wallet. This Oracle wallet file must be copied to a designated target host before its associated database instance can be cloned to that target. Use the following procedure to clone the wallet file to the target.

Perform the following configuration and verification steps on the target host.

1. Add wallet information into the sqlnet.ora file on the remote host.

```
[oracle@aie-4200f admin]$ vi sqlnet.ora
[oracle@aie-4200f admin]$ cat sqlnet.ora
ENCRYPTION_WALLET_LOCATION=
  (SOURCE=(METHOD=FILE)(METHOD_DATA=
    (DIRECTORY=/u01/app/oracle/product/11.2.0/dbhome_1/encryption_wallet/)))
```

```
[oracle@aie-4200f admin]$ mkdir -p
/u01/app/oracle/product/11.2.0/dbhome_1/encryption_wallet/
```

2. Clone the wallet files to the target host. If you are using the encryption wallet, you only have a .p12 file.

```
[oracle@aie-4200f admin]$ scp oracle@aie-4200x.us.oracle.com:/u01/app/oracle/product/11.2.0/dbhome_1/encryption_wallet/* .
oracle@aie-4200x.us.oracle.com's password:
cwallet.sso 100% 3499 3.4KB/s 00:00
ewallet.p12 100% 3421 3.3KB/s 00:00
```

```
[oracle@aie-4200f admin]$ ls
cwallet.sso  ewallet.p12  samples  shrept.lst  sqlnet.ora  tnsnames.ora  tnsnames.ora.bak
```

```
[oracle@aie-4200f admin]$ mv cwallet.sso
/u01/app/oracle/product/11.2.0/dbhome_1/encryption_wallet/
```

```
[oracle@aie-4200f admin]$ mv ewallet.p12
/u01/app/oracle/product/11.2.0/dbhome_1/encryption_wallet/
```

3. Log in to the clone instance and check the wallet information.
[oracle@aie-4200f admin]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.3.0 Production on Tue Jun 4 23:03:14 2013
Copyright (c) 1982, 2011, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> startup force
ORACLE instance started.
Total System Global Area 1269366784 bytes
Fixed Size                  2227984 bytes
Variable Size             754974960 bytes
Database Buffers          503316480 bytes
Redo Buffers                8847360 bytes
Database mounted.
Database opened.

SQL> select * from v$encryption_wallet;

WRL_TYPE
--------------------
WRL_PARAMETER
--------------------------------------------------------------------------------
STATUS
------------------
file
/u01/app/oracle/product/11.2.0/dbhome_1/encryption_wallet/
OPEN

4. Verify that the encrypted column can be seen.

SQL> conn scott/tiger
Connected.
SQL> desc empl;
Name                                      Null?    Type
----------------------------------------- -------- ----------------------------
EMPNO                                              NUMBER(4)
ENAME                                              VARCHAR2(10)
JOB                                                VARCHAR2(9)
MGR                                                NUMBER(4)
HIREDATE                                           DATE
SAL                                                NUMBER(7,2) ENCRYPT
COMM                                               NUMBER(7,2)
DEPTNO                                             NUMBER(2)

SQL> select sal from empl;

SAL
----------
800
1600
1250
2975
1250
2850
2450
3000
5000
1500
1100
SAL
---------
  950
  3000
  1300
14 rows selected.

SQL>
Appendix E: Troubleshooting Common Issues

The following issues have also been reported and listed as MOS notes under Doc ID 1522025.1, Snap Management Utility for Oracle Database – Information and Troubleshooting, on the My Oracle Support web site listed in the References section. If you do not see a listing for your issue, check the MOS notes for the latest updates to the list.

<table>
<thead>
<tr>
<th>ISSUE DESCRIPTION</th>
<th>INFORMATION/RESOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA-27102: out of memory while cloning a database.</td>
<td>If you receive ORA-27102 when cloning a snap backup or RMAN backup, there is not enough shared memory available for the database clone. Either add more shared memory or delete other databases that are running on the host or cluster. Alternatively, consider cloning the database to another host or cluster that has available space.</td>
</tr>
<tr>
<td>ORA-01034: ORACLE not available during snap backup</td>
<td>Before creating a snap backup of the database, SMU must connect to and query the database for vital information including the list of files the database is using. This error indicates that the database instance that SMU tried to connect to is shut down and not running. Restart the database instance so SMU can operate correctly. If this is a RAC database you can also modify the host account for the database to use one of the other cluster nodes that is up and running.</td>
</tr>
<tr>
<td>Cluster nodes that were down before offline snap backup are up and running afterward.</td>
<td>SMU uses the <code>srvctl stop</code> and <code>srvctl start</code> commands to temporarily shut down the database when performing an offline database. For a cluster database, if some nodes were down before the backup, they will be brought up after the backup. If you want a particular cluster node to remain down after the backup, you must use the <code>srvctl disable</code> command to disable the node so that the <code>srvctl start</code> command will not restart the node.</td>
</tr>
<tr>
<td>&quot;Auth fail&quot; or &quot;HTTP 401&quot; when performing a task.</td>
<td>When executing a task, SMU logs in to one or more host and storage systems. If the user and/or password for the account is incorrect, the task will fail, displaying either &quot;Auth fail&quot; if the account is for a Linux or Oracle Solaris storage system, or an &quot;HTTP 401&quot; error if the account is for a Windows system. Test account settings prior to executing tasks to help ensure that the account settings are correct. Use the <code>accounts test</code> command from the CLI or click the test button in the column of the account for which you want to check settings.</td>
</tr>
<tr>
<td>SMU failed on first mount of the clone of an RMAN backup – permission denied.</td>
<td>FFAS: Error creating clone using Oracle Snap Management Utility Mount failed, reason given by server: Permission denied . If root exceptions for the host are enabled using an invalid CIDR, this can be the result. Fixing the CIDR should enable the mount to succeed. Example invalid exception: root=0192.168.10.100/20.</td>
</tr>
<tr>
<td>ISSUE DESCRIPTION</td>
<td>INFORMATION/RESOLUTION</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Invalid application file layout. Remote share X has already been backed up.</td>
<td>This error indicates that the database file layout does not allow an online backup operation on this database. In order to take an online backup of the database, the datafiles and archived logs must reside in separate shares. During an online backup, snapshots of the datafile shares are taken first while the database is in backup mode. Next, the current redo logs are archived. And then snapshots of the archived log shares are taken. If, during the backup sequence, SMU detects that shares have already had snaps taken of them, it will fail the online backup task and display this error.</td>
</tr>
<tr>
<td>host X login: timeout: socket is not established.</td>
<td>This error indicates that the software could not connect to the database host (Linux or Oracle Solaris) or storage appliance. This error occurs when the database host or storage appliance are not reachable or do not respond to the connection request within a timeout period. Verify that the database host or storage appliance are up and reachable over the network and try the operation again.</td>
</tr>
<tr>
<td>Could not find all shares or shares were unavailable due to pool status.</td>
<td>This error message can occur during a task when SMU searches for the shares to operate on. A key feature SMU provides is the ability to map shares from their external attributes (mountpoint or lunguide) to their internal appliance identifier (pool/collection/project/share). This error message indicates that the shares SMU was looking for either do not exist on the Oracle ZFS Storage Appliance or are not available because the storage pool they are in is in a degraded state or other than online state. You can encounter this error if you specify the wrong storage account with a database account. In particular this error will occur when using ASM databases and the wrong storage account is specified for the database. SMU cannot determine which external storage system an iSCSI LUN is using and so will only search the storage that was linked to by the database account.</td>
</tr>
<tr>
<td>ORA-19809 occurs when creating a snap clone database.</td>
<td>This error message indicates that the size specified for the flash recovery area (FRA) is too small to support the clone database. SMU sets the size of the FRA for the clone database based on the db_recovery_file_dest_size initialization parameter of the database that was backed up. Since a snap clone is an identical copy of the source database, including the size of each redo log, the size parameter should be adequate for the clone database. To address this issue, create the clone database from a backup of the source database that has a suitable FRA size.</td>
</tr>
<tr>
<td>ISSUE DESCRIPTION</td>
<td>INFORMATION/RESOLUTION</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>The WS-Management service cannot process the request because the request contained invalid selectors for the resource.</td>
<td>This error occurs with Windows hosts when the shell session that SMU established has been idle too long. SMU uses Windows Remote Shell to connect to the host and establish a session. Windows Remote Shell will automatically log the session out if the idle timeout period expires. The software alternates issuing commands to the host and storage. It is possible for the host session to be idle while SMU sends commands to the storage. To resolve this, increase the WinRS idle timeout period to a larger value (the software requires the timeout period to be 2 hours or more). C:&gt;winrm set winrm/config/winrs @{IdleTimeout=&quot;7200000&quot;}</td>
</tr>
<tr>
<td>BUI always displays fetching data or displays it frequently.</td>
<td>The BUI is designed to refresh itself regularly so that it can display the current status of tasks and other items in the various UI panes. The amount of data to display can grow over time. Completed tasks are retained until removed or deleted by the user. It is possible to accumulate a large number of tasks that prevent the BUI from refreshing its display properly. Either delete completed tasks that are no longer needed or disable the UI refresh by modifying the global refresh settings.</td>
</tr>
<tr>
<td>The WS-Management service cannot process the request. The maximum number of concurrent operations for this user has been exceeded. Close existing operations for this user, or raise the quota for this user.</td>
<td>This error indicates that the WinRM setting MaxConcurrentOperationsPerUser is set too low. The software's recommended value for this setting is 1500. The software executes many SQL Plus, RMAN and system commands on the host while performing operations, greater than the number of commands allowed by default. To modify this setting, run the following command: C:&gt;winrm set winrm/config/service @{MaxConcurrentOperationsPerUser=&quot;1500&quot;}</td>
</tr>
<tr>
<td>Clone database task hangs when target database host is Linux running UEK kernel and dNFS is enabled in the target Oracle home.</td>
<td>This error occurs when the UEK kernel 2.6.32-300.11.1.el5uek is running on the database host. More information on this issue is available in Doc ID 1460787.1. To resolve, you must upgrade your kernel to 2.6.32-300.26.1 or disable dNFS. The software does not support the use of an oranfstab file in this release.</td>
</tr>
</tbody>
</table>
| Clone database task hangs during control file creation on Windows database host. | This error occurs because the WinRM setting MaxTimeoutms is set too low. Some of the commands SMU runs can take a while to complete. The software requires that this parameter be set to a value high enough to allow these long-running commands to complete. This error can also be verified by examining the software log for an exception like the following: "Exception in thread: "Thread-416" javax.xml.ws.soap.SOAPFaultException: The WS-Management service cannot complete the operation within the time specified in...
<table>
<thead>
<tr>
<th>ISSUE DESCRIPTION</th>
<th>INFORMATION/RESOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OperationTimeout.&quot; To address the issue, modify the setting of the MaxTimeoutMs setting and run the clone task again.  C:&gt;winrm set winrm/config @{MaxTimeoutMs=&quot;72000000&quot;}</td>
<td></td>
</tr>
<tr>
<td>No rows for datafile X in v$datafile_copy system view. This error occurs during an RMAN clone operation when SMU cannot find a row for one of the backed-up data files in the backed-up control file v$datafile_copy system view. This indicates that the data file is not a part of the backup set or the control file was backed up before the data file was backed up. SMU requires that each data file in the backup has a row in this system view so that it can calculate the maximum SCN (system change number) to recover the database to. To resolve this issue, create a valid backup that contains the data files, archived logs and control file.</td>
<td></td>
</tr>
<tr>
<td>Database already in backup mode. This error indicates that a database that SMU attempted to back up was already in backup mode. Another process or program could be backing up the database. SMU will not back up a database that is already in backup mode. If the database is not being backed up by other utilities, then the database must be taken out of backup mode manually before SMU can successfully back up the database.</td>
<td></td>
</tr>
<tr>
<td>Cannot map disk &lt;hostname</td>
<td>ip address&gt;:&lt;lun guid&gt; This error indicates that SMU could not find the clone disk on the database host or node. When cloning an ASM database, SMU clones the appropriate snapshot on the appliance to create new LUNs. SMU then uses operating system-specific commands to discover the clone LUNs from the database host or node. If the clone LUNs cannot be discovered, then SMU reports this error. The usual cause is that the appropriate iSCSI targets have not been logged into the database host or node. The software performs no SAN configuration and requires that all iSCSI targets be logged into before any ASM database clone operations are performed.</td>
</tr>
<tr>
<td>Does SMU need to communicate with Recovery catalog at main site for deploying Dev. DB with image copy (Clone) at DR site? SMU does not currently use the RMAN catalog. SMU requires that the backup shares contain a single full image copy backup. SMU will scan the backup shares and identify the control files, data files and archive logs in the backup shares. It will then snap and clone the backup shares and mount the clone shares on the target database host and proceed to configure and start a clone database that uses the files as is.</td>
<td></td>
</tr>
<tr>
<td>If the source database is RAC, should the target DB be RAC as well? No. SMU can detect if the backup is of a single instance or RAC database and will perform the appropriate processing on the clone based on whether it is targeted for a single instance or RAC environment. In other words you can create single instance or RAC clones no matter if the source is single instance or RAC.</td>
<td></td>
</tr>
<tr>
<td>ISSUE DESCRIPTION</td>
<td>INFORMATION/RESOLUTION</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Multiple operating systems (Redhat/IA Linux, SPARC/Oracle Solaris) exist at the source side. Should the same platforms be prepared for target databases?</td>
<td>In general, we recommend having the same platform. However, SMU can migrate a clone database from one operating system to another as long as both are the same Endian architecture. This means if the source database is Linux/IA you can create a clone on an Oracle Solaris/IA host. You cannot clone from little endian to big endian. So if your production environment is using SPARC/Oracle Solaris, you can only create clones on a SPARC/Oracle Solaris host.</td>
</tr>
<tr>
<td>Should the backup format be image copy? Are the files data and control needed?</td>
<td>Yes, the backup must be in image copy format. See &quot;RMAN Clone&quot; section in table 28, Quick Reference for SMU Operations Restrictions. Backup files must use the RMAN %U format specification and must contain only one control file, one or more data files and one or more archived logs. Note the sample RMAN export runblock: <code>run { set nocfau; # back up the control file explicitly allocate channel ch1 device type disk format '/backup/smu/%U'; allocate channel ch2 device type disk format '/backup/smu/%U'; allocate channel ch3 device type disk format '/backup/smu/%U'; allocate channel ch4 device type disk format '/backup/smu/%U'; backup as copy database plus archivelog; backup as copy current controlfile; }</code></td>
</tr>
<tr>
<td>WARNING: A Bean Validation provider is not present, therefore bean validation @ is disabled</td>
<td>This warning displays in the /var/opt/ORCLsmu/smu.log but has nothing to do with SMU functionality; rather, it is an ADF informational notice. It can be ignored when searching the log in troubleshooting.</td>
</tr>
</tbody>
</table>