Overview

This chapter provides an overview of Oracle Snap Management Utility for Oracle Database (SMU) and explains the general principles of application security.

Product Overview

Oracle Snap Management Utility for Oracle Database simplifies common database administrator tasks when the Oracle databases are hosted on Oracle ZFS Storage Appliances. It allows the administrator to:

- Create on-disk backups of databases using ZFS snapshots
- Restore databases from on-disk backups using ZFS rollback
- Clone databases from on-disk backups using ZFS clone
- Clone databases from RMAN backups using ZFS snapshot and clone

The software is designed to run on the administrator’s management station (Oracle Linux, Oracle Solaris or Microsoft Windows) and remotely control the database, database host and Oracle ZFS Storage Appliance during operations. The key benefit the software provides is the ability to coordinate activities between the host and storage. The software uses secure connections to the database resources using the SSH or Windows Remote Shell (HTTPS) protocols.

Basic Security Principles

The software follows these security principles:

**User and Account passwords are stored in password-protected Java keystores.**
Java keystores are encrypted so that their contents cannot be read without the keystore password.

**Connections to the SMU server are through SSH or HTTPS.**
The software command-line interface is accessed from SSH clients or `winrs.exe` with the `ssl` option. The browser user interface is accessed from web browsers using the HTTPS protocol.

**Connections to the database, database host and storage appliance are through SSH or HTTPS.**
The software connects to Oracle Linux and Oracle Solaris hosts for remote command execution using the SSH protocol. Connections to Windows hosts use the Windows Remote Management protocol using the HTTPS listener. Connections to the database use OS authentication.

**The SMU server runs as an unprivileged user on the management host.**
The software consists of a single program, which runs as an unprivileged user on Oracle Linux and Oracle Solaris hosts. On Microsoft Windows hosts the software runs as a Windows Service.
Secure Installation and Configuration

This chapter outlines how the SMU software is securely installed and configured.

Installation Overview

The latest version of the Oracle Snap Management Utility for Oracle Database is available for download from the Oracle Software Delivery Cloud. The software distribution consists of a single package for each supported operating system. The packages are in “native” package format for the operating system. The packages are installed using the standard operating system utilities. The software is secure by default; no processes or services are started during installation. The software must be manually started by the user after installation.

Resource Accounts

The software requires that the user add a set of accounts for each resource that will be accessed during operations. These are user accounts that the software uses to log in and establish a shell-type session with the resource. The software needs to be able to run privileged commands during operations. The software runs a very limited set of privileged commands. The following describes the commands and privileges that the software requires with each resource.

Database

The software automatically determines the username of the Oracle user on Oracle Linux and Oracle Solaris hosts and becomes that user when it needs to connect to and control the database. SMU connects to the database using the SYSDBA role. This role is required because the software may stop and start the database. On Microsoft Windows hosts, the software expects that the user that was specified with the database host account is the Oracle user.

Database Host

The software needs to be able to modify the filesystem table when adding new filesystem shares, create new mount points, and mount and unmount clone filesystems from the Oracle ZFS Storage Appliance. The software also needs to be able to scan the iSCSI bus and add and remove new disk devices on Oracle Linux and Oracle Solaris hosts.

Storage Appliance

The software must be able to create snapshots, roll back shares and clone shares within a project. Additionally the software must be able to destroy clone shares. It is recommended that a separate appliance user be created for the software and that this user be assigned the appropriate permissions for correct operation. The privileges for a user can be restricted to specific projects that contain the database shares that will be operated on.

Password Protection

All user and account passwords are encrypted and stored in password-protected Java keystores. The keystores and other associated data files are backed up when you back up the SMU data directory or folder on the management station.
Security Features

This chapter provides a high-level overview of the security features of the software.

Security Model

The critical security features that provide protection are:

- **Authentication** – The software requires that users log in to the SMU server before they can perform operations. Additionally, the software relies on mechanisms used by the database host and storage appliance to authenticate users specified in the account settings.

- **Authorization** – The software requires that the users specified in the resource accounts have the appropriate privileges to perform operations such as starting and stopping the database, mounting a filesystem and creating a snapshot.

- **Confidentiality** – All sensitive data used by the software is stored securely in Java keystores. The data is encrypted. Additionally, all interactions with the software and by the software occur through secure network channels such as SSH or HTTPS.

Secure Deployment Checklist

The following is a set of criteria that should be met to safely and securely deploy the software. It is strongly recommended that these requirements are followed.

**Change the SMU admin user password after first login.**

The default password for the SMU admin user is *changeit*. This password should be changed on first login. Note that if the admin password is lost, it can be reset by stopping the SMU server and setting a SMU configuration property in the *smu.conf* file.

**Create a separate storage appliance account.**

In the Oracle ZFS Storage Appliance CLI or BUI, create a separate user account specifically for use with the SMU software. Like any other user, the SMU requires a user account to gain access to the Oracle ZFS Storage Appliance. The account is created on the Oracle ZFS Storage Appliance itself. Likewise, all permissions and privileges are administered on the appliance. Use the guidelines for least privileges. At a minimum, this user must have the permissions to create snapshots, roll back shares, clone shares and destroy shares.

**Use a secure password for the user and account passwords.**

When choosing a password for the resource accounts used by SMU, pick a string of at least eight characters. Longer passwords introduce a greater number of possibilities, making it harder to guess with each additional character. Also consider the complexity of the password. To introduce a higher level of complexity, the password should contain characters from each of the following categories:

1. Lowercase alpha: a-z
2. Uppercase alpha: A-Z
3. Numeric: 0-9
4. Special characters: ! @ # $ % ^ & * ( )
Do not repeat any characters or use passwords that represent names of people, places, things, or events.

Use the HTTPS Windows Remote Management listener with a self-signed or CA signed SSL certificate.

The software connects to Windows hosts using the Windows Remote Management protocol. The software supports both HTTP and HTTPS connections. When using HTTPS connections, an SSL certificate with the extended usage key indicating server authentication must be used. A self-signed certificate or Certificate Authority (CA)-signed certificate can be used.