

Chapter 5

Integrating Sun ONE Directory Server

Sun ONE Directory Server is a software product by Sun Microsystems, Inc. that provides a central repository for storing and managing identity profiles, access privileges, and application and network resource information. This chapter describes how to integrate Sun ONE Directory Server with Juniper Networks routers and the SRC software.

For information about compatibility of this SRC release with Sun ONE Directory Server releases, see the *SRC-PE Release Notes*.

Topics in this chapter include:

- Overview of Sun ONE Directory Server Integration on page 45
- Integrating the Sun ONE Directory with the SRC Software on page 47
- Starting Sun ONE Directory Server on page 49
- Stopping Sun ONE Directory Server on page 50
- Restarting Sun ONE Directory Server on page 50
- Backing Up the Sun ONE Database on page 50
- Restoring the Sun ONE Database on page 51

Overview of Sun ONE Directory Server Integration

You can integrate the Sun ONE Directory Server product into your SRC environment by installing an SRC add-on package and then installing Sun ONE Directory Server as specified in this chapter. Sun ONE Directory Server is based on industry-standard LDAP and provides advanced security features, carrier-grade scalability, performance, and availability. Sun ONE acts as a central repository for the consolidation of subscriber profiles.

You can use the information stored in Sun ONE Directory Server for the authentication and authorization of subscribers to enable secure access to enterprise and Internet services. Sun ONE helps to ensure that appropriate access control policies are enforced across all communities, applications, and services on a global basis.

About the Sun ONE Add-On Package

The Sun ONE Directory Server add-on package for the SRC software is called UMCiDSa. This package provides integration files for Sun ONE Directory Server versions 5.1 and 5.2:

- An *sdx.inf* file, which integrates with Sun ONE's silent installation feature.
 - For Sun ONE Directory Server versions 5.1—*/opt/UMC/conf/iDS/SunOne5.1/sdx.inf*
 - Sun ONE Directory Server versions 5.2—*/opt/UMC/conf/iDS/SunOne5.2/sdx.inf*
- A load script and files in LDAP Data Interchange Format (LDIF) to integrate Sun ONE Directory Server with the SRC software in the */opt/UMC/conf/iDS* directory.

Silent Installation for Sun ONE Directory Server

Sun ONE's silent installation feature allows Sun ONE software to be embedded with the SRC software through an *sdx.inf* file specific to the version of Sun ONE Directory Server that is being installed. No user intervention is required during the setup process. Table 7 describes important setup script information provided in an *sdx.inf* file.

Table 7: Information Provided for the Sun ONE Setup Script

Configuration Property	Value
Installation path	<i>/opt/UMC/iDS</i>
Directory configuration administrator (Sun ONE entity)	admin
Password for directory configuration administrator	admin
LDAP port to be used for directory instance	389
Server identifier (Sun ONE specific). The directory instance is installed in the path:	sdx <i>/opt/UMC/iDS/slaped-sdx</i>
Suffix for new LDAP directory instance	<i>o = umc</i>
Identifier for superadministrator	<i>cn = umcAdmin, o = umc</i>
Password for superadministrator	admin123
Administrator's port	6666



NOTE: The uid-uniqueness plug-in is not enabled within the initial configuration of the Sun ONE Directory Server software. Because the SRC software does not require a globally unique user ID, this feature should remain disabled.

Load Script to Integrate Sun ONE Directory Server

The **load** script performs the following tasks:

- Configures the password storage mechanism not to use encryption.

If you use Merit AAA Server (RADIUS), note that it requires that passwords be stored as clear text, the **load** script changes a setting to not store the password in an encrypted manner.

- Extends the LDAP schema to:
 - Add SDX schema requirements
 - Index SDX attributes
 - Create the directory infrastructure for SDX entries
 - Load access control information

Sun One Directory Server stores the access control information in the `aci` attribute, which is available for all directory entries. The load script processes the *access.ldif file* to add required access control information.

- Lets you load sample data

The **load** script is designed to work with Sun ONE Directory Server 5.1 and 5.2. For version 5.1, you enter the command with the **5.1** option:

```
load 5.1
```

For version 5.2, you enter the command without any options:

```
load
```

Integrating the Sun ONE Directory with the SRC Software

The tasks to integrate the Sun ONE Directory Server with the SRC software are:

1. Installing the Solaris operating system and the patches that the Sun ONE directory server requires. See the documentation for Sun ONE directory Server for details.
2. Installing the Sun ONE Directory Add-On Package on page 48
3. Configuring an Instance of Sun ONE Directory Server on page 48

Before you can integrate the Sun ONE Directory Server software with the SRC software, you must have access to the Sun ONE Directory Server software; the Sun ONE Directory Server software is not included with your SRC software. See the *SRC-PE Release Notes* for information about the versions of Sun ONE Directory Server and the associated service packs supported.

Obtain the software by downloading the Sun ONE Directory Server software from the Sun Microsystems Web site at:

<http://www.sun.com/download>

Installing the Sun ONE Directory Add-On Package

You must install the Sun ONE Directory add-on package for the SRC software before you install Sun One Directory Server. For information about installing the package, see *SRC-PE Getting Started Guide, Chapter 33, Installing the SRC Software on a Solaris Platform*.

Configuring an Instance of Sun ONE Directory Server

You must create a new instance of the Sun ONE Directory to integrate the Sun ONE Directory Server software with the SRC software.

To create an instance of Sun ONE Directory and integrate it with the SRC software:

1. Uncompress the archive file that you downloaded from the Sun Microsystems Web site by executing the command:

```
gzip -dc <filename>.tar.gz | tar xvf -
```

where `<filename>` is the name of the TAR file.

2. Move to the directory that contains the expanded files.

For example, if you saved the downloaded file into the directory `/tmp/DS`, enter:

```
cd /tmp/DS
```

3. Enter the command appropriate to the version of Sun ONE Directory Server to install an instance of the directory by using an `sdx.inf` file.

- For Sun One Directory Server 5.1:

```
./setup -s -f /opt/UMC/conf/SunOne5.1/sdx.inf
```

- For Sun One Directory Server 5.2:

```
./setup --nodisplay --noconsole --state /opt/UMC/conf/SunOne5.2/sdx.inf
```

4. Move to the following directory:

```
/opt/UMC/conf/iDS
```

5. Enter the command appropriate to the version of Sun ONE Directory Server to run a **load** script.

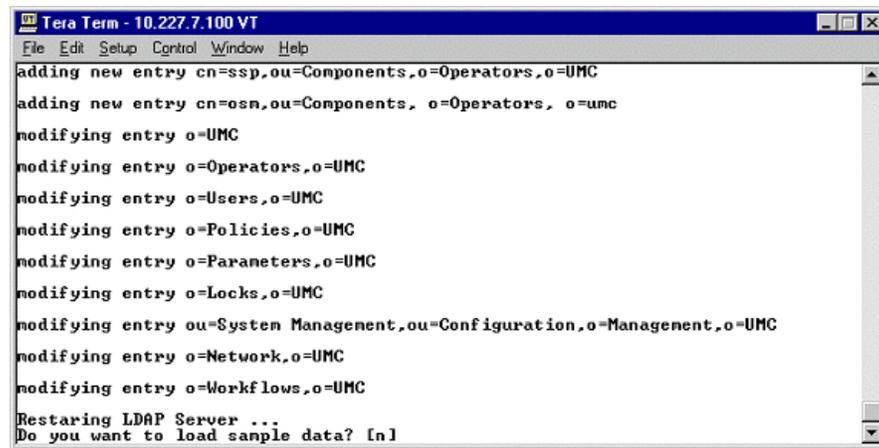
- For Sun One Directory Server 5.1:

./load 5.1

- For Sun One Directory Server 5.2:

./load

After the script updates the schema, loads the directory infrastructure, and creates the access controls, the script prompts you to load the sample data. An example is shown in the following window.



```

Tera Term - 10.227.7.100 VT
File Edit Setup Control Window Help
adding new entry cn=ssp,ou=Components,o=Operators,o=UMC
adding new entry cn=osn,ou=Components,o=Operators,o=umc
modifying entry o=UMC
modifying entry o=Operators,o=UMC
modifying entry o=Users,o=UMC
modifying entry o=Policies,o=UMC
modifying entry o=Parameters,o=UMC
modifying entry o=Locks,o=UMC
modifying entry ou=System Management,ou=Configuration,o=Management,o=UMC
modifying entry o=Network,o=UMC
modifying entry o=Workflows,o=UMC
Restarting LDAP Server ...
Do you want to load sample data? [n]

```

After the script finishes running, SRC components can use the Sun ONE Directory Server.

Starting Sun ONE Directory Server

To start Sun ONE Directory Server:

1. On the Sun ONE Directory Server host, log in as **root** or as an authorized nonroot admin user.
2. Start the Sun ONE Directory Server from its installation directory.

/opt/UMC/conf/iDS/ldap start

Stopping Sun ONE Directory Server

To stop Sun ONE Directory Server:

1. On the Sun ONE Directory Server host, log in as `root` or as an authorized nonroot admin user.
2. Stop the Sun ONE Directory Server from its installation directory.

```
/opt/UMC/conf/iDS/ldap stop
```

Restarting Sun ONE Directory Server

To restart Sun ONE Directory Server:

1. On the Sun ONE Directory Server host, log in as `root` or as an authorized nonroot admin user.
2. Restart the Sun ONE Directory Server from its installation directory.

```
/opt/UMC/conf/iDS/ldap restart
```

Backing Up the Sun ONE Database

You can manually back up the database for any directory you have installed. For information about migrating a directory database to another host, see *SRC-PE Getting Started Guide, Chapter 39, Upgrading the SRC Software on a Solaris Platform*.

To back up the Sun ONE (formerly iPlanet) database:

1. Log in as `root`.
2. Access the database folder.

```
cd /opt/UMC/iDS/slaped-sdx
```

3. Back up the database.

```
./db2bak
```

This script makes a copy of the database and stores it in the following location:

```
/opt/UMC/iDS/slaped-sdx/bak/YYYY_MM_DD_HHMMSS
```

The backup directory identifies the date (YYYY_MM_DD) and time (HHMMSS) when the backup was created.

Restoring the Sun ONE Database

You can manually restore the database for any directory you have installed. For information about migrating a directory database to another host, see *SRC-PE Getting Started Guide, Chapter 39, Upgrading the SRC Software on a Solaris Platform*.

To restore the Sun ONE database:

1. Log in as `root`.

2. Access the database folder.

```
cd /opt/UMC/iDS/slappd-sdx
```

3. Verify that the Sun ONE Directory Server is shut down. If it is not, shut it down.

```
./stop-slappd
```

4. Make sure you know the exact backup directory.

5. Run the `bak2db` script by typing:

```
./bak2db /opt/UMC/iDS/slappd-sdx/bak/YYYY_MM_DD_HHMMSS
```

where `YYYY_MM_DD_HHMMSS` identify the date and time when the database backup was created.

6. Start the Sun ONE server.

```
./start-slappd
```

We recommend that you restart SRC components after restoring directory data from a backup, to ensure that the restored database is used.

