Configuring an LDAP Directory for SESM Deployments

This appendix describes how to install and configure LDAP directories to work with SESM. SESM is verified to run with the following directories:

- Novell eDirectory Versions 8.5 and 8.7. (eDirectory Version 8.7 runs on Solaris Version 7 or 8; it does not run on Solaris Version 2.6.)
- iPlanet Version 5.x on Solaris Version 2.6. (iPlanet Version 5.1 is recommended.)
- Sun ONE Directory Server Version 5.1 SP1 on Solaris Version 8. (Sun ONE does not run on Solaris Version 2.6.)

Topics in this appendix are:

NDS Installation and Configuration Requirements

This section describes how to install and configure Novell eDirectory Version 8.5 or 8.7 to work with SESM. Topics are:

Summary of Administrative Access to NDS

When you complete the procedures described here, the NDS directory is configured as follows:

- The following SESM container exists in the NDS directory:
  - Tree name: sesm
  - Server context: ou=sesm.o=cisco
- The following attribute on the SESM LDAP group object is set to true (required).
  - On NDS Version 8.5, the Allow Clear Text Passwords attribute
  - On NDS Version 8.7, the Require TLS for Simple Binds with Password attribute

- Access to the SESM container through ConsoleOne is granted with the following distinguished name (dn) in the format shown:
  - name: cn=admin.ou=sesm.o=cisco
  - password: value you specified during the NDS installation

  This administrative user has all required permissions to update the NDS directory schema and also to create and modify objects in the SESM container.
- When configuring SESM and SPE, use the following format for distinguished name:

  ```
  cn=admin,ou=sesm,o=cisco
  ```

Installation and Configuration Procedures

To install and configure NDS to work with SESM, perform the following steps. These instructions assume that you are installing NDS on a Solaris machine.

Step 1 Log on as super user.

Step 2 Create an NDS directory on the Solaris machine. A typical location is /usr/nds.

Step 3 If you have an NDS tar file, place it into the directory you just created and expand it.

Step 4 Run the installation file, which is located in:

```
/usr/nds/NDS8.5/Solaris/setup/nds-install
```

Step 5 The installation program prompts you to read and accept the License agreement.

Step 6 The installation program prompts you to choose the components to install, as follows:

```
1)NDS Server
2)Adminisration Utilities
3)Management Console for NDS (ConsoleOne)
```

In most cases, you should install all three components. To do so, enter:

```
1 2 3
```

Step 7 The installation program prompts you for the location of the license files. Enter:

```
/usr/nds/NDS8.5/licensefiles
```

Note Refer to the NDS documentation if you do not have the license files.

Step 8 The installation program installs the requested packages. Then it asks whether or not you want to install the Java Runtime Environment (JRE). The JRE is required for ConsoleOne, the NDS management console. If you do not already have a suitable JRE installed on the machine, enter:

```
yes
```

Step 9 The installation program opens the NDS server configuration file (/etc/ndscfg.inp) in a text editor. Use the editor to enter the following required information. Use the values shown below to ensure compatibility with SESM installation and sample data defaults:

```
Admin Name and Context: cn=admin.ou=sesm.o=cisco
Tree Name: sesm
Create NDS Tree: YES
Server Context: ou=sesm.o=cisco
```

Two additional fields (server IP address and Database Files directory) are optional. You do not need to enter values for them.

Step 10 Save the configuration file and quit the editor.

Step 11 The installation program prompts you for a password for the admin user. Use any password.

Note The SESM installation program prompts you for the administrator name (admin) and this password when you install the SPE component.

Step 12 The installation program concludes by prompting you to manually edit two environment variables:

```
PATH=$PATH:/usr/ldaptools/bin
MANPATH=$MANPATH:/usr/ldaptools/man
```

Step 13 Go to the following section to enable the Allow Clear Text Passwords (NDS Version 8.5) or Require TLS for Simple Binds with Password (NDS Version 8.7) attribute. This setting is required.

Setting Allow Clear Text Passwords or Require TLS for Simple Binds with Password

For SESM to work with NDS, the Allow Clear Text Passwords (NDS Version 8.5) or Require Transport Layer Security (TLS) for Simple Binds with Password (NDS Version 8.7) attribute must be true. This NDS option allows transmission of bind requests that include passwords over nonencrypted connections. By default, only passwords exchanged over SSL connections are encrypted. The option is a property of the LDAP Group object of a server.

To set Allow Clear Text Passwords or Require TLS for Simple Binds with Password, follow these procedures:

Step 1 Start ConsoleOne. Run the following file:

```
/usr/ConsoleOne/bin/ConsoleOne &
```

Step 2 Log in (authenticate) to the NDS Directory as follows:

- If the Login window does not appear:
  - Click on the **NDS** icon in the tree.
  - From the menu, choose **File** > **Authenticate**.
- In the Login window, use the following values if you used all of the standard defaults when you installed the directory:

```
Login name: admin
Password: cisco
Tree: SESM
Context: ou=sesm.o=cisco
```

- Click **Enter**.

Upon successful authentication, the .SESM. icon appears in the right-hand panel.

Step 3 Enable the required attribute as follows:

- In the left panel, expand the NDS tree to the sesm object level:

```
NDS
    .SESM.
        cisco
            sesm
```

- In the left panel, click **sesm** to select it.
- In the right panel, right-click the **LDAP Group object**.
- Choose **Properties** from the pop-up menu.
- In the **General** tab, in the middle of the window, check the **Allow Clear Text Passwords** (NDS Version 8.5) or **Require TLS for Simple Binds with Password** (NDS Version 8.7) option.
- Click **Apply**.
- Click **Close**.

Step 4 Exit ConsoleOne and proceed to SESM installation.

Sun ONE and iPlanet Installation and Configuration Requirements

This section describes how to install and configure Sun ONE and iPlanet to work with SESM. Topics are:

Summary of Administrative Access to Sun ONE and iPlanet

On completion of the instructions in the following section, your Sun ONE or iPlanet directory is configured as follows:

- The following administrative user has all required permissions to update the directory schema:
  - name: cn=Directory Manager
  - password: value you specify during the directory installation
- The following SESM container exists in the directory:
  - Tree name: sesm
  - Server context: ou=sesm.o=cisco
- The following administrative user has all required permissions to create and modify objects in the SESM container.
  - name: uid=*yourAdmin*,ou=sesm,o=cisco

    where *yourAdmin* is a value you specify during container creation
  - password: a value you specify during container creation

Installation and Configuration Instructions

To install and configure Sun ONE or iPlanet to work with SESM, perform the following steps. These instructions assume that you are installing iPlanet Version 5.0 on a Solaris 2.6 system or Sun ONE Version 5.1 SP1 on a Solaris Version 8 system.

Step 1 Log on as superuser.

Step 2 If you have a tar file, expand it.

Step 3 Execute the setup file. Follow the instructions in the setup program.

Step 4 When the program displays the following prompt, select the **iPlanet Servers** option.

```
1. iPlanet Servers
    Installs iPlanet Servers with the integrated iPlanet Console onto your computer.
2. iPlanet Console
    Installs iPlanet Console as a stand-alone Java application on your computer.
```

Step 5 In response to subsequent prompts asking you which components to install, select all components.

Step 6 At the following prompt, we recommend that you enter the standard port 389, rather than accepting the random default port. You must know this port number later in this procedure and also during SESM installation.

```
Directory server network port[nnnnn]: 389
```

Step 7 At the following prompt, accept the default value of **admin**.

```
iPlanet configuration directory server
administrator ID [admin]:
Password:
Password (again):
```

Enter the password of your choice. This user name and password has privileges to update the directory schema. You must enter this admin ID and password later in this procedure and also during SESM installation.

Step 8 At the following prompt, enter the value **o=cisco**.

```
Suffix [dc=]:o=cisco
```

Step 9 At the following prompt, accept the default value of **Directory Manager**.

```
Directory Manager DN [cn=Directory Manager]:
Password:
Password (again):
```

Enter the password of your choice. This user name and password has privileges to add objects to the cisco container you created in the previous step. You must enter this Directory Manager DN and password later in this procedure and also during SESM installation.

Step 10 At the following prompt, enter any port number. The configuration examples later in this procedure use the value 390.

```
Administration port [15197]:390
```

Step 11 At the following prompt, enter a user name or accept the default value (root).

```
Run Administration Server as [root]:
```

The installation process is complete. After successful installation, the iPlanet server might start automatically. If not, start it as described in the next step.

Step 12 Start the directory server by executing the following:

```
/usr/iplanet/servers/start-admin
```

Step 13 Start the console by executing the following:

```
/usr/iplanet/servers/startconsole
```

A logon window appears.

Step 14 Log on as follows:

```
User ID:cn=Directory Manager
Password:
AdminURL:http//hostname:390
```

The iPlanet Console window appears.

Step 15 Expand the folders in the console window until the Directory Server object appears. Select **Directory Server** and click **Open** at the top right corner of the window.

An iPlanet Directory Server window appears.

Step 16 Right-click the **cisco** folder. Choose **New** > **Org Unit** from the pop-up menu.

Step 17 In the Name field, enter **sesm** and click **OK**.

Step 18 Right-click the **sesm** object. Choose **New** > **User** from the pop-up menu. A Create New User window appears.

Step 19 Enter appropriate values in the following fields. In the UserID field, enter **admin**.

```
First Name:
Last Name:
Common Name:
UserID: admin
Password:
```

Click **OK**.

Step 20 Right-click the **sesm** object. Choose **Set Access Permissions** from the pop-up menu. The Manage Access Control window for ou=sesm,o=cisco appears.

Step 21 Click **New**. The Edit ACI window for ou=sesm,o=cisco appears.

Step 22 Enter any value for ACI Name. Click **Add**. The Add User & Group window appears.

Step 23 Enter **admin** in the search field. Click **Search**: The admin user appears in the top window.

Step 24 Select **admin** and click **Add**. The admin user appears in the bottom window. Click **OK**.

Step 25 Click **Targets**. Click **This Entry**. Click **OK**.

Step 26 Click **OK** in the Manage Access Control window.

Step 27 Exit iPlanet or Sun ONE and proceed to the SESM installation.