

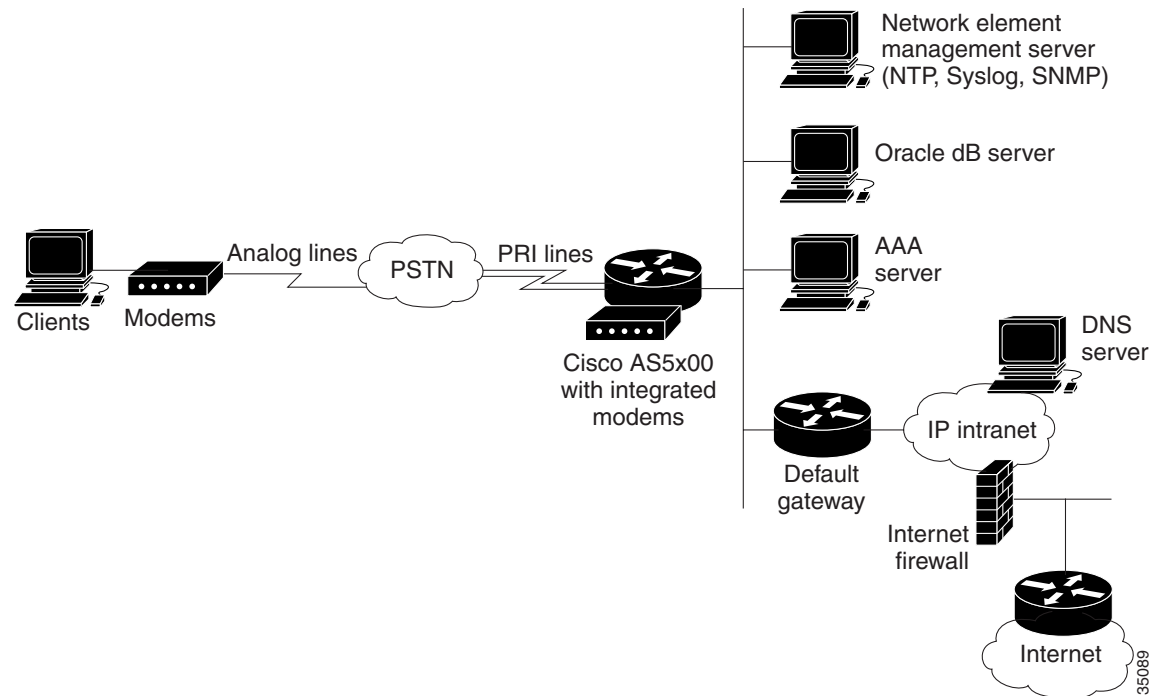
## Implementing Cisco AAA Servers

This chapter describes the basic process of installing CiscoSecure for UNIX (CSU). See Chapter 1, “Cisco AAA Case Study Overview” for information regarding this case study’s network requirements and environment details for this case study. Figure 3-1 illustrates the general networking environment in which this CSU is implemented.

These sections focus on the following topics:

- 3.1 Installing CiscoSecure for UNIX with Oracle
- 3.1.4 Creating and Verifying Basic User Profile

**Figure 3-1** AAA-Based, Secure Network Access Scenario



## 3.1 Installing CiscoSecure for UNIX with Oracle

These processes help you to install CiscoSecure for UNIX:

- 3.1.1 Creating Oracle Tablespace
- 3.1.2 Verifying the Oracle Database Instance
- 3.1.3 Installing CiscoSecure for UNIX
- 3.1.4 Creating and Verifying Basic User Profile

### 3.1.1 Creating Oracle Tablespace

You must create an Oracle tablespace with a minimum size of 200 MB. The notes listed in this section are for reference.



#### Note

Ensure that an experienced Oracle database administrator (DBA) tunes and configures the database.

For detailed Oracle installation notes, go to the following location:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/cs\\_unx/csbsdoc.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csbsdoc.htm)

Example of creating a Oracle tablespace:

```
<CSUserver>$su - oracle
Sun Microsystems Inc. SunOS 5.5.1 Generic May 1996
<CSUserver>$ORACLE_HOME/bin/svrmgr1

Oracle Server Manager Release 2.3.4.0.0 - Production

Copyright (c) Oracle Corporation 1994, 1995. All rights reserved.

Oracle7 Server Release 7.3.4.0.1 - Production
With the distributed option
PL/SQL Release 2.3.4.0.0 - Production

SVRMGR>connect internal
Connected.
SVRMGR>create tablespace cstb datafile '/export/home/ORADATA/cs.dbf' size 200m;
Statement processed.
SVRMGR>create user csecure identified by csecure default tablespace cstb;
Statement processed.
SVRMGR>grant dba to csecure identified by csecure;
Statement processed.
SVRMGR>exit
Server Manager complete.
```

## 3.1.2 Verifying the Oracle Database Instance

Before you install CiscoSecure for UNIX, make sure the Oracle server is running and you have the following five pieces of information:

- The Oracle user account for CiscoSecure (csecure)
- The password for the Oracle account (csecure)
- TNS service name for the Oracle server (ciscosj)
- The location of \$ORACLE\_HOME (/opt/oracle/product/7.3.4)
- The number of Connections to use for ORACLE RDBMS (50)

**Step 1** To verify the software directory environment variable (*\$ORACLE\_HOME*) where Oracle is installed, enter the following command. Log in to the *\$ORACLE\_HOME* as follows:

```
<CSUser>$env | grep ORACLE_HOME
ORACLE_HOME=/opt/oracle/product/7.3.4
```



**Note** This environment variable should have been configured during Oracle installation by the DBA.

**Step 2** On the Oracle server, verify that *SMON* (a mandatory Oracle background process) is running by entering the following command:

```
<CSUser>$ps -ef | grep smon
oracle 819 1 0 Feb 26 ? 0:00 ora_smon_ciscosj
```

The command returns the *ora\_smon\_<SID>* process if the server is running. Notice the database instance specification of *ciscosj*. If the server is down, log in with the Oracle UNIX account (in this case, with username of *csecure* and password of *csecure*) and start the database by using Server Manager (*svrmgrl*) and Oracle listener (*lsnrctl*) as follows:

```
<CSUser>$ORACLE_HOME/bin/svrmgrl
SVRMGR>connect internal
SVRMGR>startup
ORACLE instance started.
Total System Global Area 4576056 bytes
Fixed Size 39816 bytes
Variable Size 4118448 bytes
Database Buffers 409600 bytes
Redo Buffers 8192 bytes
Database mounted.
Database opened.
```

```

<CSUserver>$$ORACLE_HOME/bin/lsnrctl start
LSNRCTL for Solaris:Version 2.3.4.0.0 - Production on 12-APR-00 09:40:46

Copyright (c) Oracle Corporation 1994. All rights reserved.

Starting /opt/oracle/product/7.3.4/bin/tnslsnr:please wait...

TNSLSNR for Solaris:Version 2.3.4.0.0 - Production
System parameter file is /opt/oracle/product/7.3.4/network/admin/listener.ora
Log messages written to /opt/oracle/product/7.3.4/network/log/listener.log
Listening on:(ADDRESS=(PROTOCOL=ipc) (DEV=10) (KEY=ciscoaus))
Listening on:(ADDRESS=(PROTOCOL=ipc) (DEV=13) (KEY=PNPKEY))
Listening on:(ADDRESS=(PROTOCOL=tcp) (DEV=15) (HOST=172.22.53.204) (PORT=1521))

Connecting to (ADDRESS=(PROTOCOL=IPC) (KEY=ciscosj))
STATUS of the LISTENER
-----
Alias                     LISTENER
Version                   TNSLSNR for Solaris:Version 2.3.4.0.0 - Production
Start Date                12-APR-00 09:40:50
Uptime                    0 days 0 hr. 0 min. 0 sec
Trace Level               off
Security                  OFF
SNMP                      OFF
Listener Parameter File  /opt/oracle/product/7.3.4/network/admin/listener.ora
Listener Log File        /opt/oracle/product/7.3.4/network/log/listener.log
Services Summary...
   ciscoaus                has 1 service handler(s)
The command completed successfully

```

**Step 3** To verify that the Oracle database account information is created for CiscoSecure by the DBA, enter Security Manager using the **sqlplus** process:

```

<CSUserver>$$sqlplus csecure/csecure@ciscosj

SQL>select * from user_sys_privs;

USERNAME                                PRIVILEGE                                ADM
-----                                -
CSECURE                                UNLIMITED TABLESPACE                    NO

```



**Note** Ensure that the assigned resource role/privilege for the username and password is as shown.

The command returns a table with a column listing the privileges granted to the Oracle database account. The default tablespace assigned to the Oracle database account must be at least 200MB. The size is verified by the installation script.

**Step 4** To confirm *tnsnames* service is operating correctly, invoke the **tnsping** utility as follows:

```

<CSUserver>$$ORACLE_HOME/bin/tnsping ciscosj

TNS Ping Utility for Solaris: Version 2.3.4.0.0 - Production on 29-FEB-00 09:25:28

Copyright (c) Oracle Corporation 1995. All rights reserved.

Attempting to contact (ADDRESS=(PROTOCOL=TCP) (Host=CSUserver) (Port=1521))
OK (80 msec)

```

- Step 5** Ensure the number of Oracle RDBMS connections assigned to CiscoSecure is less than the PROCESSES variable defined in the *initcscosj.ora* file. This parameter specifies the maximum number of user processes that can simultaneously connect to an Oracle Server. If the value for PROCESSES is set to 20, then only 13 or 14 concurrent connections can be assigned to CiscoSecure. For this case study, at least four of the connections are reserved for mandatory background server processes. In addition, the PROCESSES variable is set to 50 and the number of Oracle RDBMS connections is set to 50 during the installation.
- 

### 3.1.3 Installing CiscoSecure for UNIX

The general steps and output that follow apply to the installation dialog for CiscoSecure for UNIX (CSU) on a Sun Solaris workstation. Installation consists of the following steps:

1. Start the CSU installation process by invoking the pkgadd program.
2. Configure CSU logging by editing */etc/syslog.conf* to enable AAA syslog function:
3. Create */var/log/csuslog* file.
4. Configure the AAA server for maximum level debugging.
5. Restart the AAA server.
6. Restart the syslog daemon.

**Step 1** Start the CSU installation process by invoking the *pkgadd* program.

The process that follows illustrates the general installation sequence. Extraneous output was omitted where noted for brevity.



**Note** The following installation process requires approximately 20 minutes.

```
<CSUserver>$pkgadd -d CiscoSecure-2.3.3.solaris
```

```
The following packages are available:
```

```
 1 CSCEacs      CiscoSecure Access Control Software
                   (sun4) 2.3(3)
```

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:1
```

```
Processing package instance <CSCEacs> from </opt/install/cisocsecure/CiscoSecure
-2.3.3.solaris>
```

```
CiscoSecure Access Control Software
(sun4) 2.3(3)
```

```
Copyright(c) 1996-1999 Cisco Systems, Inc.
CiscoSecure Access Control Server
Version 2.3(3)
All Rights Reserved.
```

```
Copyright (c) 1994-1999 Netscape Communications Corporation
Copyright (c) 1988-1999 Sybase, Inc.
Trade Mark WebLogic, Inc.
```

```
Notice:
```

```
By using this product, you agree to be bound by the terms of
the license supplied with this product. If you do not agree
to these terms, promptly return the unused product, manuals,
related equipment, and hardware (with proof of purchase) to
the place of purchase for a full refund.
```

```
To install this product, you must agree to accept the terms
of the enclosed license [accept=y,exit=n,exit=q]: y
```

```
checking patches...
```

```
*****
* Notice:
* This installation program saves your Database files from a previous *
* CiscoSecure install. If you have not installed CiscoSecure before, *
* you should answer YES to the next question. If you have performed *
* a 'package remove' and are installing a new version of CiscoSecure *
* and want to retain your previous Database files, you should answer *
* NO to the next question.
*****
```

```
Is this a new install (y/n/q) (default: yes, q to quit)?y
```

```
Enter the directory name in which to install CiscoSecure [?,q]/opt/cisocsecure
```

```

IP Address to use for CiscoSecure (default: 172.23.25.41) [?,q]

If the hostname of this server is not the same as its fully qualified domain
name (FQDN), enter the FQDN, e.g., www.cisco.com. Otherwise, press enter
to use the default (default: CSUser) [?,q]

Enter the AAA Server License key (default: <none>) [?,q]

Enter the TACACS+ NAS name to use (default: <none>) [?,q]

Enter the TACACS+ NAS Secret key (default: SECRET12345) [?,q]ciscorules

Select any or all Token Cards to use
 1 CryptoCard
 2 Secure-Computing      SafeWord
 3 SDI                    SDI Token Card

Enter selection (default: none) [?,??,q]:

Choose Database
 1 SQLAnywhere          Sybase SQL Anywhere
 2 ORACLE               Oracle Enterprise
 3 SYBASE               Sybase Enterprise

Enter selection (default: SQLAnywhere) [?,??,q]:2

Enter the username for the ORACLE DB account [?,q]csecure

Enter the password for the ORACLE DB account [?,q]csecure

Enter the TNS service name for the Oracle Server [?,q]ciscosj

Enter the ORACLE_HOME directory [?,q]/opt/oracle/product/7.3.4

Enter an available TCP/IP Port to be reserved for the CiscoSecure DB Server
process (default: 9900) [0-65535,?,q]

Enter a unique name for the CiscoSecure DB Server Process (default:
CSdbServer) [?,q]

Enter the number of Connections to use for ORACLE RDBMS (default: 4) [?,q]50

Enter the directory Path to use for the AAA server profile caching
(default: /, q to quit)?

        Modify any selections below?

New CiscoSecure Install                YES
CiscoSecure Directory                  /opt/ciscosecure
CiscoSecure IP Address                  172.23.25.41
CiscoSecure Web Server Name             CSUser
Profile Cache Directory                 /
AAA License Key                         <none>
TACACS+ NAS Name                       <none>
TACACS+ NAS Secret Key                 SECRET12345
Token Cards selected                    none
Data Base                               ORACLE
DB User Account Name                   csecure
DB User Account Passwd                 csecure
Oracle TNS Name                        ciscosj
Oracle Home                            /opt/oracle/product/7.3.4
CiscoSecure DB Server IP Address        172.23.25.41
CiscoSecure DB Server Port              9900
CiscoSecure DB Server Proc Name         CSdbServer

```

DB Server Connections 50

Modify any values [y,n,q]: **n**

cs\_install.log being written to /tmp directory

Using </opt/ciscosecure> as the package base directory.

## Processing package information.

## Processing system information.

6 package pathnames are already properly installed.

## Verifying disk space requirements.

## Checking for conflicts with packages already installed.

## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user permission during the process of installing this package.

Do you want to continue with the installation of <CSCEacs> [y,n,?] **y**

Installing CiscoSecure Access Control Software as <CSCEacs>

## Executing preinstall script.

## Installing part 1 of 1.




---

**Note** Process output is omitted at this point because it is not relevant to the installation task presented in this chapter.

---

[ verifying class <TSERVER> ]

## Executing postinstall script.

Creating the initial database tables and views.....

Loading properties from /opt/ciscosecure/config/CSConfig.ini

Finished loading properties.

Data Source = ORACLE

Driver Type = JDBC-Weblogic-Oracle URL = jdbc:weblogic:oracle:ciscosj username = csecure password = \*\*\*\*\*

Connected to jdbc:weblogic:oracle:ciscosj

Driver Weblogic, Inc. Java-OCI JDBC Driver (weblogicoci26)

Version 2.5.4

```
sql = select tablespace_name, floor(sum(bytes)/(1024*1024)) from sys.dba_free_space
where tablespace_name = (select default_tablespace from sys.dba_users where
username = USER) group by tablespace_name
```

Total free space in CSTB tablespace is 199 MB.

Creating /opt/ciscosecure/utills/sql.scripts/ora\_init.sql%

Executing SQL statements..



**Note** Process output is omitted at this point because it is not relevant to the installation task presented in this chapter.

Successfully done.

Initializing RADIUS data in the database.....

Loading properties from /opt/ciscosecure/config/CSConfig.ini

Finished loading properties.

Data Source = ORACLE

Driver Type = JDBC-Weblogic-Oracle URL = jdbc:weblogic:oracle:ciscosj username = csecure password = \*\*\*\*\*

Connected to jdbc:weblogic:oracle:ciscosj

Driver Weblogic, Inc. Java-OCI JDBC Driver (weblogicoci26)

Version 2.5.4

Radius data version: 23

Adding SERVER\_LIST

Adding DICTIONARY\_LIST

Adding SERVER.172.23.25.41

Adding DICTIONARY.IETF

Adding DICTIONARY.Cisco

Adding DICTIONARY.Ascend

Adding DICTIONARY.Cisco11.1

Adding DICTIONARY.Cisco11.2

Adding DICTIONARY.Cisco11.3

Adding DICTIONARY.Ascend5

No update to dictionary list

Update radius version: INSERT INTO cs\_id (id, type) VALUES (?, ?)

Successfully done.

Installation is complete. However, further configuration may be necessary. For more information on the steps necessary to finish configuration, read the /opt/ciscosecure/DOCS/README.txt file.

Results of this install are saved in the /tmp/cs\_install.log file and in /opt/ciscosecure/logfiles/cs\_install.log.

NOTE: For AAA Server tuning, refer to

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/cs\\_unx/csu23rg/app\\_b.htm#xtocid192003](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csu23rg/app_b.htm#xtocid192003)

Installation of <CSCEacs> was successful.

**Step 2** Configure CSU logging by editing */etc/syslog.conf* to enable AAA syslog function:

Enter the following command:

```
#added by rbrown@cisco.com on 02/28/00
local0.debug /var/log/csuslog
```



**Note** Do not use whitespace to separate the above statements in */etc/syslog.conf*. Use only tabs.

**Step 3** Create */var/log/csuslog* file.

Enter the **touch** command to create the *csulog* file.

```
<CSUser>$touch /var/log/csuslog;chmod 777 csuslog
```

**Step 4** Configure the AAA server for maximum level debugging.

Modify */opt/ciscosecure/config/CSU.cfg* as follows:

```
NUMBER config_logging_configuration = 0x7fffffff
```

**Step 5** Restart the AAA server.

Enter the following command to restart the AAA server:

```
<CSUser>$/etc/rc0.d/K80CiscoSecure
```

Stopping CiscoSecure Processes:

```
CiscoSecure AutoRestart Stopped
Fast Track Server Stopped
Fast Track Admin Program Stopped
Acme Server Stopped
AAA Server Stopped
DBServer Stopped
```

```
<CSUser>$/etc/rc2.d/S80CiscoSecure
```

Starting CiscoSecure Processes:

```
Fast Track Admin Started
FastTrack Server (Delayed Start)
DBServer Started
AAA Server starts in 15 Seconds: 123456789012345
AAA Server Started
Acme Server Started
Cisco AutoRestart started
```

**Step 6** Restart the *syslog* daemon.

Enter the follow command to restart the *syslog* daemon:

```
<CSUser>$ps -ef |grep syslog
  root   150      1  0   Feb 26 ?           0:00 /usr/sbin/syslogd
<CSUser>$kill -HUP 150
```

## 3.1.4 Creating and Verifying Basic User Profile

These processes help you to accomplish basic user profile creation and verification:

1. Create user *csu\_test*.
2. Verify user *csu\_test*.
3. Configure the router for basic authentication.
4. Log in to the router and verify user access.
5. Review the AAA server log.

**Step 1** Create user *csu\_test*.

Enter the following commands to add the user *csu\_test*:

```
<CSUserver>$/opt/ciscosecure/CLI/AddProfile -p 9900 -u csu_test -pw des,ciscorocks
Profile Successfully Added
```

**Step 2** Verify user *csu\_test*.

Enter the following commands to verify settings for user *csu\_test*:

```
<CSUserver>$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u csu_test
User Profile Information
user = csu_test{
profile_id = 18
profile_cycle = 1
password = des "*****"
}
```

**Step 3** Configure the router for basic authentication.

Log in to the router and include the following commands:

```
aaa new-model
aaa authentication login default group tacacs+ local

tacacs-server host 172.22.53.201 key ciscorules
```

**Step 4** Log in to the router and verify user access.

Enter the user name and password:

```
Username:csu_test
Password:<password>
```

**Step 5** Review the AAA server log.

Enter the **tail** command to assess the *csulog* file:



**Note** This CSU log fragment illustrates user *csu\_test* being authenticated and permitted privilege level 15 access.

```
<CSUserver>$tail -f /var/log/csulog
Feb 29 16:52:28 CSUserver last message repeated 20 times1
Feb 29 16:52:30 CSUserver CiscoSecure: DEBUG - ACCOUNTING request (55d45ae8)
Feb 29 16:52:30 CSUserver CiscoSecure: DEBUG - acct_token_cache_session_add_del: user:
csu_test
Feb 29 16:52:30 CSUserver CiscoSecure: DEBUG - acct_token_cache_session_add_del: user:
csu_test
Feb 29 16:52:30 CSUserver CiscoSecure: DEBUG - AUTHENTICATION START request (8f414e3e)
Feb 29 16:52:30 CSUserver CiscoSecure: DEBUG -
Feb 29 16:52:30 CSUserver User Access Verification
Feb 29 16:52:30 CSUserver CiscoSecure: DEBUG - Username:
Feb 29 16:52:31 CSUserver CiscoSecure: WARNING - No swap files/partitions allocated
Feb 29 16:52:33 CSUserver CiscoSecure: DEBUG - AUTHENTICATION CONTINUE request (8f414e3e)
Feb 29 16:52:33 CSUserver CiscoSecure: DEBUG - Password:
Feb 29 16:52:35 CSUserver CiscoSecure: DEBUG - AUTHENTICATION CONTINUE request (8f414e3e)
Feb 29 16:52:35 CSUserver CiscoSecure: DEBUG - Authentication - LOGIN successful; [NAS =
coe-ccie-35.cisco.com, Port = tty2, User = csu_test, Priv = 15]
```

