

Troubleshooting Cisco Secure ACS for UNIX

Document ID: 19002

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Troubleshoot the Installation

- Troubleshoot the Initial Installation
- Verify the Installation

Post-Installation Issues

- Collection of General CSUnix Information
- Browser Issues
- Troubleshoot AAA Server Processes
- Troubleshoot Individual User/Group Problems
- Beginning GUI (Acme Web Server) Debug
- Advanced GUI (Netscape Fast Track Web Server) Debug
- General Database Troubleshooting
- Troubleshoot the Oracle Database
- Troubleshoot the NAS Debug
- Troubleshooting Commands

Related Information

Introduction

This document assists you with diagnosing common problems with Cisco Secure Access Control Server (ACS) for UNIX (CSUnix). It also describes the information to collect when you report CSUnix problems to Cisco Technical Support. In the examples provided within this document, the CSUnix base installation directory is designated as \$BASEDIR since this can vary from system to system.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on all versions of Cisco Secure ACS for UNIX.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Troubleshoot the Installation

Troubleshoot the Initial Installation

Most issues that occur when you install CSUnix can be attributed to either an unsupported operating system (OS), database, or browser. Supported configurations are always listed in the installation documentation for the version in question and are also summarized in the Cisco Secure ACS UNIX Compatibility Matrix.

Forward and reverse name resolution should work prior to installation, as this example shows:

```
# hostname
rtp-evergreen

# nslookup rtp-evergreen
Server:  redclay2.cisco.com
Address: 172.18.125.3

Non-authoritative answer:
Name:    rtp-evergreen.cisco.com
Address: 172.18.124.114

# nslookup 172.18.124.114
Server:  redclay2.cisco.com
Address: 172.18.125.3

Name:    rtp-evergreen.cisco.com
Address: 172.18.124.114

# nslookup rtp-evergreen.cisco.com
Server:  redclay2.cisco.com
Address: 172.18.125.3

Non-authoritative answer:
Name:    rtp-evergreen.cisco.com
Address: 172.18.124.114
```

Interoperability of CSUnix has not been tested and is not supported with software other than what is cited in the installation guide. If other software is installed, application port conflicts can cause CSUnix installation problems. It is recommended that CSUnix is the only application that runs on the server to avoid these issues. CSUnix uses these ports:

- DBServer: TCP/9900 and TCP/9901
- AAA Server: TCP/49 (TACACS+), UDP/1645, and UDP/1646 (RADIUS)
- Acme WebServer: TCP/9090
- Netscape Fastrack Server: TCP/80 and TCP/64000
- SSL: TCP/443 (component is optional)
- Oracle: TCP/1521 (component is optional)

If there are issues when installing CSUnix on a supported platform, gather this information to help determine the issue:

- A copy of the \$BASEDIR/logfiles/cs_install.log file.
- The output from these UNIX commands:

- ◆ **uname -a**
- ◆ **showrev -p**
- ◆ **pkginfo**
- ◆ **netstat -an**
- ◆ **hostname**

- ◆ nslookup <ip>
- ◆ nslookup <FQDN>
- ◆ nslookup <hostname>

Note: You must be logged in as user *root* when you install CSUnix.

Verify the Installation

After CSUnix installs, the CSUnix services are not automatically started. Issue `/etc/rc2.d/S80CiscoSecure` or `$BASEDIR/utills/scs` to start the services. If by some means the services were started, issue `/etc/rc0.d/K80CiscoSecure` or `$BASEDIR/utills/kcs` to stop them and issue `/etc/rc2.d/S80CiscoSecure` or `$BASEDIR/utills/scs` to restart them.

These messages should appear:

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

You can also verify that all the processes are started by running `$BASEDIR/utills/psg`. You should see at least one process started for each service, as this example shows.

```
# ./opt/CSCEacs/utills/psg
<database process>:
SQL Anywhere Engine:
root 18519 1 /opt/CSCEacs/SYBSsa50/bin/dbeng50 -ud -ga -n csecure
-N 17

<database process>:
CiscoSecure DB Server Process:
root 18506 1 /opt/CSCEacs/java/bin/sparc/native_threads/java
-ms10m -mx64m cisco.ciscosecure

<advanced gui>:
Netscape Web Server Processes:
nobody 18562 1 ./ns-httpd -d
/opt/CSCEacs/ns-home/httpd-rtp-cherry/config
nobody 18566 18562 ./ns-httpd -d
/opt/CSCEacs/ns-home/httpd-rtp-cherry/config
nobody 18564 18562 ./ns-httpd -d
/opt/CSCEacs/ns-home/httpd-rtp-cherry/config
nobody 18565 18562 ./ns-httpd -d
/opt/CSCEacs/ns-home/httpd-rtp-cherry/config
nobody 18563 18562 ./ns-httpd -d
/opt/CSCEacs/ns-home/httpd-rtp-cherry/config

<advanced gui>:
Netscape Web Admin Processes:
root 18500 18498 /opt/CSCEacs/ns-home/admserv/ns-admin -d
/opt/CSCEacs/ns-home/admserv
root 18498 1 /opt/CSCEacs/ns-home/admserv/ns-admin -d
/opt/CSCEacs/ns-home/admserv

<beginning gui>:
Acme Web Server Process:
root 18541 1 /opt/CSCEacs/java/bin/sparc/native_threads/java
-mx100m Acme.Serve.Serve
```

```

<AAA server process>:
    CiscoSecure AAA Server Process [2.3(6)]:
    root 18539 1 /opt/CSCEacs/CSU/CiscoSecure -f
    /opt/CSCEacs/config/CSU.cfg

<autorestart process>:
    CiscoSecure Auto Re-Start Process:
    root 18544 1 /bin/sh /opt/CSCEacs/bin/CiscoAuto.sh 30 skip
    /opt/CSCEacs

```

If one or more processes fail to start, the errors are recorded in the `$BASEDIR/logfiles/cs_startup.log` file. This log file also tells you if your license key is invalid or has expired. This is an example of a log file that shows an invalid license warning:

```

# cat cs_startup.log
warning: daemon is running as super-user
startup: listening to port 64000 as root
warning: commands will be executed using /bin/sh
job 1004369319.a at Mon Oct 29 07:28:39 2001
CiscoSecure INFO - libdb.so: protocol version 1.1

CiscoSecure INFO - Establishing All Connections with DB Server
Debug Initializer

CiscoSecure INFO - libdb.so: Connections to Database Server
established.
CiscoSecure WARNING - Insecure configuration: Encryption key is
too short - NAS <default>
CiscoSecure WARNING - invalid license token ""
CiscoSecure INFO - Using default of 4 ports
startup: listening to port 80 as nobody
Mon Oct 29 07:28:56 PST 2001 rtp-evergreen CiscoSecure: INFO -
CiscoSecure Auto
Re-Start Process Started.....

```

In this example, CSUnix still allows four connections (or authentications) to occur. All subsequent authentications fail until the system is restarted. The only way to resolve this issue is to obtain a valid license key which is based upon your host system's `hostid`.

Note: The warning `Insecure configuration:Encryption key too short` signifies that a defined network access server (NAS) has a server key value that is blank or too short. This does not mean the NAS does not authenticate. However, for security reasons, it is recommended that you use a longer server key.

Post-Installation Issues

The debug process and information that needs to be collected depends on what part of the system is failing and if the system formerly worked and then started to fail. At a minimum, the information in the section is needed.

Collection of General CSUnix Information

Use the `$BASEDIR/CSU/CiscoSecure -v` command to retrieve your CSUnix version information. Issue these commands to retrieve information on the Solaris OS version and patches used:

- `uname -a`
- `showrev -p`
- `pkginfo`

Use these commands and resources to gather information on your Solaris system:

- Gather the output of these UNIX commands:
 - ◆ **netstat -an**
 - ◆ **hostname**
 - ◆ **nslookup <ip>**
 - ◆ **nslookup <FQDN>**
 - ◆ **nslookup <hostname>**
- Issue the **df -k** command to view disk space information.
- Issue the **/usr/openwin/bin/wsinfo** command to view memory and workstation information.
- Issue the **/usr/sbin/prtconf** command to view the print system configuration.
- Issue the **psrinfo -v** to view computer processing unit (CPU) information.
- Other applications/services running on your machine such as CiscoWorks or Oracle.
- Output of the **\$BASEDIR/utills/psg** command.
- Determine if the protocol currently running is either Terminal Access Controller Access Control System Plus (TACACS+) or Remote Access Dial-In User Service (RADIUS).
- Configuration files for the CSUnix application (BASEDIR\$/configCSU.cfg and BASEDIR\$/config/CSConfig.ini).
- Router and server **debug** logs.
- Information on whether the function in question was previously working and any recent changes to the system.

Browser Issues

Supported browsers are listed in the installation instructions for your specific version. The initial login screen is accessed by entering **http://<ip_of_box>/cs**.

The initial CiscoSecure Logon screen is known as the beginning graphical user interface (GUI). The default username/password is **superuser/changeme**. Most operations such as manipulating users and passwords can be performed on the beginning GUI. If there is a need to modify user or group profiles by accessing the advanced GUI, hit the **Advanced** button to arrive at the CiscoSecure Administrator screen (advanced GUI).

If you experience problems with access to either GUI, check for these:

- Can the GUIs be accessed from the local box on which CSUnix is installed?
- Does forward and reverse name resolution work on the CSUnix box and the remote box that is accessing CSUnix?
- Does the **show java console** box on the browser provide information?
- Is there a Security error on the advanced GUI?
- Does local administration or administration from a few work-stations succeed for some but not others?

Security Error on Advanced GUI

In CSUnix version 2.3.x and later, there is a new feature known as Validate Clients (ValidClients). By default, this feature is enabled, but is not configured to allow access to the advanced GUI. If you try to access the advanced features with this feature enabled, but not configured, you will receive a security error. To resolve this issue, either disable the feature or configure hosts that are allowed to access the GUI.

Complete these steps to disable ValidClients:

1. Locate the CSConfig.ini file in the \$BASEDIR/config directory of the CSUnix ACS 2.3 installation.

2. Back-up the CSConfig.ini file and insert or edit these lines in the [ValidClients] section of the CSConfig.ini file:

```
[ValidClients]
ID_num = my_wrk_station
.
.
.
ValidateClients = false
```

3. After you edit the CSConfig.ini file, recycle CSUnix to apply the changes.

Follow this example to enable a subset of ValidClients to connect:

- This example shows two workstations, with the fully qualified domain names (FQDNs) of ws-barrylee and ws-pameagan, being authorized to access the CSUnix administration tools. The setting **ValidateClients = true** stops any workstation not specifically listed in the [ValidClients] section from accessing the CSUnix Web pages or the command-line interface (CLI):

```
[ValidClients]
100 = ws-barrylee
120 = ws-pameagan
ValidateClients = true
```

Remote Administration Failure

Make sure that you use a compatible browser with Java enabled. If you do not use a compatible browser you may experience problems with scroll bars not functioning and problems re-initializing the server after changes are made in the servers or NAS section of the GUI.

Another possible browser issue can be caused by having proxy on. You should not use an HTTP proxy when you browse to the CSUnix server. With proxy on, you may encounter issues when you access the GUI or security errors when you attempt to access the advanced GUI.

Your remote workstation should have the same date/time set as the CSUnix server. Variations of over three minutes may cause issues since the date/time is used to encrypt the communication between the remote client and the server. You can determine if this is the issue by looking at the \$BASEDIR/logfiles/cs_startup.log file. If you see Service ID (SID) decryption errors, synchronize the time/date between the systems. Also check the timezone (TZ) variable in the env output on the UNIX station.

Domain Name Server (DNS) Issues

A common remote browser problem, which is difficult to troubleshoot, involves DNS issues. When you remotely administer the CSUnix box, you may input the hostname or the IP address of the server to gain access to the CSUnix server. Whatever you type into your browser is resolved by your local DNS server. This is fine for accessing the beginning GUI. For instance, you may enter something similar to **http://10.10.10.120/cs/**. However, once you get to the main CSUnix screen, the URL may read **http://acsserver.acme.com:9090/....** This is fine as long as the CSUnix server name you configured during installation is **acsserver.acme.com** and not **acsserver**. When you access the advanced GUI, the hostname in the URL must match, or be resolved to the CSUnix server name in order for Java to run correctly. You can check the CSUnix server name in one of these two places:

- \$BASEDIR/logfiles/cs_install.log
- \$BASEDIR/ns-home

For \$BASEDIR/ns-home, you should have a directory with `httpd-servername` specified. For example, `.../httpd-acme`. This example uses an **nslookup** command on the IP address of the CSUnix server to see if it

returns an exact match to this hostname:

```
# nslookup 10.10.10.120
```

If the name lookup returns a server name that does not match the CSUnix server name, or does not return a name, you need to update your local DNS server. If you do not run a name resolution service, then update the /etc/hosts table on the CSUnix server and the corresponding hosts file on the remote station if it uses local resolution.

Troubleshoot AAA Server Processes

Setting-up the CSUnix debug to write to a file is necessary if the authentication process itself fails. These steps describe how to setup debugging on CSUnix to write to file csuslog in the /var/log directory.

Note: If you use RADIUS, the server debug must also be turned on. This is done in the browser by selecting **Advanced GUI > Server** and checking **Debugging = Enabled**. Alternatively, at the command line, you can enter '**\$BASEDIR/CLI/UpdateProfile -p 9900 -u SERVER.###.# -a DebuggingEnabled=Yes**' where ###.# is the IP address of the server.

1. Back up the \$BASEDIR/config/CSU.cfg file before you change this line which tells CSUnix how much debugging to do from the default:

```
NUMBER config_logging_configuration = 0x7E;  
to 0x7FFFFFFF which turns on all possible debugging:  
NUMBER config_logging_configuration = 0x7FFFFFFF;
```

2. The additional line

```
NUMBER config_system_logging_level = 0x80;
```

in CSU.cfg, sends the debugging information to syslog local0.

3. Modify the /etc/syslog.conf file by adding the entry **local0.debug /var/log/csuslog**.

Note: The Solaris file syntax requires that you press the **tab** and not the **space** key between '.debug' and /var.

4. Make sure the /var/log/csuslog file exists and is writable.
5. Recycle syslog.pid to re-read the configuration file. To do this, enter **kill -HUP `cat /etc/syslog.pid`**.
6. Enter this to recycle the Cisco Secure server:

```
/etc/rc0.d/K80CiscoSecure  
/etc/rc2.d/S80CiscoSecure
```

You should now have application messages logging to /var/log/csuslog. This file can grow to be rather large. Therefore, troubleshooting with this file may require that you look at the tail of the file for the most recent information. For example, to read the last 100 lines enter:

```
# tail -100 /var/log/csuslog
```

Troubleshoot Individual User/Group Problems

If the problem is limited to a particular user or group, profiling information on the failing user or group is necessary. For example:

- Enter this command to gather profile information on the failing user:

```
$BASEDIR/CLI/ViewProfile -p 9900 -u <user>
```

- Enter this command to gather profile information on the failing group:

```
$BASEDIR/CLI/ViewProfile -p 9900 -g <group>
```

- Enter this command to gather profile information on the failing server:

```
$BASEDIR/CLI/ViewProfile -p 9900 -u <SERVER.###.##.>
```

Note: `###.##.` is the IP address of the machine on which CSUnix is installed.

Beginning GUI (Acme Web Server) Debug

The beginning GUI runs on the Acme Web server. To obtain Acme Web debug information, make changes to these files:

1. Set these variables in `$BASEDIR/FastAdmin/turbo.conf`:

```
DEBUG_LEVEL = 5
DEBUG_THRESHOLD = 0
```

2. Set this variable in `$BASEDIR/FastAdmin/servlets.conf`:

```
set logging=true
```

The resulting output goes into the `$BASEDIR/logfiles/cs_startup.log` file.

Advanced GUI (Netscape Fast Track Web Server) Debug

The advanced GUI runs on the Netscape Fast Track Web server. Obtaining debug information for the Netscape Fast Track Web server requires that the **debug** command be enabled on the Acme Web server. Command output also goes into `$BASEDIR/logfiles/cs_startup.log` file.

Additional access and error logs of the Netscape server are stored in the `$BASEDIR/ns-home/httpd-$SERVERNAME/logs` directory.

General Database Troubleshooting

Complete these steps to turn on database debugging if your database runs but you suspect that there are intermittent abnormalities:

1. Enter `$BASEDIR/DBClient/DBClient -p 9900`.
2. Enter `admin_Commands`.
3. Enter `df 0 15`.
4. Hit **enter** twice to turn on the protocol and accounting manager trace. This causes detailed debugging output to go to `$BASEDIR/logfiles/<server_log>`. When the services are recycled, the debugging reverts to off.

If the database does not start, back up the `$BASEDIR/bin/DBServer.sh` file and change this line in file `$BASEDIR/bin/DBServer.sh` from:

```
eval exec $BASEDIR/bin/detach $JBASE/bin/java -ms10m -mx64m
cisco.ciscosecure.dbserver.Main -cfile $BASEDIR/config/CSConfig.ini
```

to:

```
eval exec $BASEDIR/bin/detach $JBASE/bin/java -ms10m -mx64m
cisco.ciscosecure.dbserver.Main -cfile $BASEDIR/config/CSConfig.ini -DEBUG
```

0:1:2:3:4:5:6:7:8:9:10:11:12:13:14:15:16:17:18:19

Note: The options added should be in the same line.

Recycle the CSUnix services. This results in additional debug information going to the \$BASEDIR/logfiles directory.

Additional Information

This list is additional information needed to troubleshoot database issues:

- The database being used (SQLAnywhere (default), Oracle, or Sybase).
- The version of the database if using Oracle or Sybase.
- A copy of these log files from the \$BASEDIR/logfiles/ directory:

- ◆ csdb_date.log
- ◆ dbserver.log
- ◆ cs_startup.log
- ◆ cs_install.log

- The number of users in the database. This can be obtained by issuing this command:

```
# BASEDIR/utils/bin/ExecSql "select count ( * ) from cs_user_profile"
```

- Is the replication being used (if any) master–master or master–snapshot? This is only valid for Oracle or Sybase.

Troubleshoot the Oracle Database

Complete these steps to troubleshoot the Oracle database.

1. Check to see if the Oracle listener process runs along with the other Oracle processes by running **ps -ef | grep oracle** to return the PID for the tnslnsr process. For example:

```
ps -ef | grep oracle
oracle 2901 1 /u01/app/oracle/product/805/bin/tnslnsr LISTENER -inherit
```

2. If the **tnslnsr** process runs, issue the **lsnrctl** command from the \$ORACLE_HOME/bin directory.
3. At the LSNRCTL> prompt, issue the **status** sub–command to find out if the listener is running.
4. Issue the **show/services** command to identify if the service is running.

Note: The tnsnames.ora file must have the SID parameter defined for the service name similar to the line from this example:

```
(CONNECT_DATA = (SID = 0E80)
```

5. Check to see if the **tnslnsr** process accesses the correct tnsnames.ora file. The status command in the LSNRCTL> prompt shows the listener parameter file. The tnsnames.ora file is usually present in the same directory.
6. Issue the **tnsping** command to check if the address and port information in the tnsnames.ora configuration file are correct:

```
$ORACLE_HOME/bin/tnsping <service_name>
```

Note: The <service_name> is obtained from the tnsnames.ora file, for example:

```
SERVICE_NAME = POPC10
```

Note: Therefore, the command is:

```
tnsping POPC10
```

7. Make sure the **env** command output shows these environmental variables defined:

- ◆ ORACLE_BASE
- ◆ ORACLE_HOME
- ◆ ORACLE_SID
- ◆ LD_LIBRARY_PATH

Troubleshoot the NAS Debug

When you obtain debugs from a Cisco router, it is essential to turn on system date/timestamps so that router logs can be correlated with CSUnix system debugs. To enable these services, enter these commands in the global configuration mode of the router:

```
service timestamps debug datetime msec
service timestamps log datetime msec
```

Issue these **show** commands to gather information on the product platform, version, featureset, and configuration:

```
show version
show run
```

Issue these **debug** commands from the router to troubleshoot AAA issues:

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug ppp authentication
debug ppp negotiation
debug tacacs -or- debug radius
```

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

- **show version** Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.
 - **show run** Displays the source IP address that is bound to the interface.
 - **debug aaa accounting** Displays information on accountable events as they occur.
 - **debug aaa authentication** Displays information on AAA/TACACS+ authentication.
 - **debug aaa authorization** Display information on AAA/TACACS+ authorization.
 - **debug ppp authentication** Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
 - **debug ppp negotiation** Displays Point-to-Point Protocol (PPP) packets sent during PPP startup, where PPP options are negotiated.
 - **debug tacacs** Displays information associated with the TACACS.
 - **debug radius** Displays detailed debugging information associated with the RADIUS.
-

Related Information

- [Cisco Secure ACS for UNIX Support Page](#)
 - [Documentation for Cisco Secure ACS for UNIX](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 14, 2009

Document ID: 19002
