Troubleshooting Cisco Prime Access Registrar

This chapter provides information about techniques used when troubleshooting Cisco Access Registrar (Prime Access Registrar) and highlights common problems.

This chapter contains the following sections:

- Gathering Basic Information
- Troubleshooting Quick Checks
- aregcmd and Cisco Prime Access Registrar Configuration
- RADIUS Request Processing
- Other Troubleshooting Techniques and Resources
- Checking Prime Access Registrar Server Health Status

Gathering Basic Information

Table 28-1 lists UNIX commands that provide basic and essential information to help you understand the Prime Access Registrar installation environment.

Table 28-1 UNIX Commands to Gather Information

UNIX Command	Information Returned
/usr/bin/uname -r	Solaris release level
/usr/bin/uname -i	Machine hardware name
/usr/bin/uname -v	Solaris version
/usr/bin/uname -a	All system information including hostname, operating system type and release, machine model and type
/usr/sbin/prtconf	System configuration information including memory capacity, machine type, and peripheral equipment
/usr/sbin/df -k	File system disk space usage including partitions, capacity, and space used
/usr/bin/ps -ef	Currently running processes

Table 28-1 UNIX Commands to Gather Information (continued)

UNIX Command	Information Returned
/usr/sbin/psinfo -v	Information about processors
/usr/bin/pkginfo -l CSCOar	Software package information about Prime Access Registrar version number and installation directory

Note More information about these commands and their options is available using the **man** command in a terminal window on the Sun workstation.

Troubleshooting Quick Checks

Many of the most common problems can be diagnosed by doing the following:

- Check disk space
- Check for resource conflicts
- Check the Prime Access Registrar log files

Disk Space

Running out of disk space can cause a number of problems including:

- Failure to process RADIUS requests
- Parts of the Prime Access Registrar configuration *disappearing* in **aregcmd**
- Failure to log into **aregcmd**

Check that the Prime Access Registrar installation partition (**$INSTALL**) and **/tmp** are not at capacity.

Resource Conflicts

Resource conflicts are a common reason for the Cisco Prime Access Registrar server failing to start. The most common resource conflicts are the following:

- Cisco Network Registrar is running on the Prime Access Registrar server
- Another application is also using ports 1645 and 1646
- A network management application is using the Sun SNMP Agent

No Co-Existence With Cisco Network Registrar

Cisco Network Registrar cannot coexist on a machine running Prime Access Registrar for this reason. You can determine if CNR is running by entering the following command line in a terminal window:

pkginfo | grep -i “network registrar”

Port Conflicts

The default ports used by the Prime Access Registrar server are ports 1645 and 1646. You should check to determine that no other applications are listening on the same ports as Prime Access Registrar.

You can check to see which TCP ports are in use by entering the following command line:

netstat -aP tcp

You can check to see which UDP ports are in use by entering the following command line:

netstat -aP udp

Note If you configure the Prime Access Registrar server to use ports other than the default, you will have to specifically add ports 1645 and 1646 if you want to also use those ports.

Server Running Sun SNMP Agent

If you plan to use the Prime Access Registrar server's SNMP agent, you cannot use the Sun Microsystems SNMP agent that comes with the Solaris operating system.

Cisco Prime Access Registrar Log Files

Examining the Prime Access Registrar log files can help you diagnose most Prime Access Registrar issues. By default, the Prime Access Registrar log files are located in **/opt/CSCOar/logs**. Table 28-2 lists the Prime Access Registrar log files and the information stored in each log.

Table 28-2 Prime Access Registrar Log Files

Log File	Information Recorded
agent_server_1_log	Log of the server agent process
ar-status	Log of Prime Access Registrar stop and start using the **arserver** utility
aregcmd_log	Log of commands executed in aregcmd (very useful for tracing the steps that took place before a problem occurred)
config_mcd_1_log	Log of the mcd internal database
name_radius_1_log	Log of the radius server process
name_radius_1_trace	Debugging output of RADIUS request processing (only generated when the trace level, set in **aregcmd**, is greater than zero)

Modifying File Sizes for Agent Server and MCD Server Logs

The two parameters added to the **car.conf** file under **$BASEDIR/conf** affect the **agent_server_logs** and **config_mcd_server_logs logs** files:

- AGENT_SERVER_LOG_SIZE (10 MB by default)

- AGENT_SERVER_LOG_FILES (2 by default)

You will find these new parameters at the beginning of the **car.conf** file. When the log file size reaches the value set in AGENT_SERVER_LOG_SIZE, a rollover of the **agent_server_log_file** occurs. The value set in AGENT_SERVER_LOG_FILES specifies the number of log files to be created.

Using xtail to Monitor Log File Activity

A useful way of monitoring all of the log files is to run **xtail**, a utility provided with Prime Access Registrar. The **xtail** program monitors one or more files and displays all data written to a file since command invocation.

Run **xtail** in a dedicated terminal window. It is very useful for monitoring multiple logfiles simultaneously, such as with a command line like the following:

```
xtail $INSTALL/logs/*
```

Note Cisco AR 4.1.5 and later include the millisecond field in the logs' timestamp.

Modifying the Trace Level

By modifying the trace level, you can gather more detailed information in the log files about what is happening in the Prime Access Registrar server. There are five different trace levels. Each higher trace level also includes the information logged using lower trace levels. The different trace levels provide the following information:

- Level 0—No tracing occurs
- Level 1—Indicates when a packet is sent or received and when a status change occurs in a remote server (RADIUS Proxy and LDAP)
- Level 2—Information includes the following:
  - Which services and session managers are used to process
  - Which client and vendor objects are being used to process a packet
  - More details about remote servers (RADIUS Proxy and LDAP), packet transmission, and timeouts
  - Details about poorly-formed packets.
- Level 3—Information includes the following:
  - Tracing of errors in Tcl scripts when referencing invalid RADIUS attributes
  - Which scripts have been run
  - Details about local userlist processing
- Level 4—Information includes the following:
  - Advanced duplication detection processing
  - Details about creating, updating, and deleting sessions
  - Tracing of all APIs called during the running of a script
- Level 5—Provides information about policy engine operations

Installation and Server Process Start-up

The installation process installs the Prime Access Registrar software to the specified installation directory and then starts the server processes. This process rarely fails but the following checks should always be performed:

- Ensure that there is an **installation success message** at the end of the **pkgadd** dialog, otherwise check the dialog for the problem
- Follow the installation instructions carefully especially when performing an upgrade. For example, when upgrading to 1.6R1, 1.6R2, or 1.6R3, a post-installation upgrade script needs to be run
- Pay attention to the information included in README files

At the end of a successful installation, **arstatus** should show the following four server processes:

> $INSTALL/usrbin/arstatus

```
AR RADIUS server running    (pid: 6285)
AR MCD lock manager running (pid: 6284)
AR MCD server running       (pid: 6283)
AR Server Agent running     (pid: 6277)
```

If any of the above processes are not displayed, check the log file of the failed process to determine the reason. The MCD processes might fail to start if Cisco Network Registrar is installed on the same machine.

The manual method of starting and stopping the Prime Access Registrar processes is using the **arserver** utility.

To start Prime Access Registrar processes: **arserver start**

To stop Prime Access Registrar processes: **arserver stop**

To restart Prime Access Registrar processes: **arserver restart**

aregcmd and Cisco Prime Access Registrar Configuration

While troubleshooting, you should always use the **aregcmd** command **trace** to turn on tracing. With tracing active, Prime Access Registrar generates debugging output to the log file **name_radius_1_trace**.The syntax is:

trace [<server>] [<level>]

When you do not specify a server, Prime Access Registrar sets the trace level for all servers in the current cluster. When you do not specify a trace level, the currently set level is used. The default trace level is 0.

Running and Stopped States

Prime Access Registrar can be in two states, running or stopped. In either state, all four Prime Access Registrar processes remain running. The state of Prime Access Registrar will be displayed when logging into **aregcmd** or by using the **aregcmd status** command:

status

```
Server 'Radius' is Running, its health is 10 out of 10\
```

The **start** and **stop** commands allow Prime Access Registrar to move between states. **Reload** is equivalent to a **stop** followed by a **start** if Prime Access Registrar is already running, and just a **start** if it is already stopped.

stop

```
Stopping Server 'Radius'...
Server 'Radius' is Stopped
```

start

```
Starting Server 'Radius'...
Server 'Radius' is Running, its health is 10 out of 10
```

reload

```
Reloading Server 'Radius'...
Server 'Radius' is Running, its health is 10 out of 10
```

During the transition from running to stopped, Prime Access Registrar stops processing new RADIUS requests and releases resources such memory, network and database connections and open files.

During the transition from stopped to running, Prime Access Registrar reverses this process by opening a connection with its internal database, reading configuration data, claiming memory, establishing network connections, opening files, and initializing scripts. During this transition, problems can occur. Prime Access Registrar might fail to start and display the following:

reload

```
Reloading Server 'Radius'...
310 Command failed
```

Prime Access Registrar failed to move from stopped state to running:

status

```
Server 'Radius' is Stopped
```

This might occur for a number of reasons including the following:

- An invalid configuration
- Insufficient memory
- Listening ports already in use by another application
- Unable to open files
- Unable to initialize scripts

Check the **name_radius_1_log** file for the one of these indications.

RADIUS Request Processing

The main technique for troubleshooting RADIUS request processing in Prime Access Registrar is to examine the **name_radius_1_trace** log file with the trace level set to 5. Most issues are fairly self-explanatory. Some issues that can arise are as follows:

- Prime Access Registrar has marked a remote server as ***down***
- A resource manager has run out of resources (for example, user or group session limit has been reached or no more IP addresses are available)
- A configuration error (such as an accounting service not being set)
- A run time error in a script

Some issues are not immediately evident from the log files though, such as the following:

- Failure to save or reload Prime Access Registrar after a configuration change
- Prime Access Registrar is not listening on the correct UDP ports for RADIUS requests

Other Troubleshooting Techniques and Resources

aregcmd Stats Command

The **aregcmd** command **stats** provides statistics on request processing.

--> stats

```
Global Statistics for Radius:
serverStartTime = Tue Oct  2 10:28:02 2012
serverResetTime = Tue Oct  2 20:25:12 2012
serverState = Running
totalPacketsInPool = 1024
totalPacketsReceived = 0
totalPacketsSent = 0
totalRequests = 0
totalResponses = 0
totalAccessRequests = 0
totalAccessAccepts = 0
totalAccessChallenges = 0
totalAccessRejects = 0
totalAccessResponses = 0
totalAccountingRequests = 0
totalAccountingResponses = 0
totalStatusServerRequests = 0
totalAscendIPAAllocateRequests = 0
totalAscendIPAAllocateResponses = 0
totalAscendIPAReleaseRequests = 0
totalAscendIPAReleaseResponses = 0
totalUSRNASRebootRequests = 0
totalUSRNASRebootResponses = 0
totalUSRResourceFreeRequests = 0
totalUSRResourceFreeResponses = 0
```

```
totalUSRQueryResourceRequests = 0
totalUSRQueryResourceResponses = 0
totalUSRQueryReclaimRequests = 0
totalUSRQueryReclaimResponses = 0
totalPacketsInUse = 0
totalPacketsDrained = 0
totalPacketsDropped = 0
totalPayloadDecryptionFailures = 0
```

Core Files

A core file in the Prime Access Registrar installation directory is an indication that Prime Access Registrar has crashed and restarted. Check that the radius server process generated the core file using the UNIX **file** command:

> file core

```
core:           ELF 32-bit MSB core file SPARC Version 1, from 'radius'
```

Check the timestamp on the core file and look for corresponding log messages in the **name_radius_1_log** file in **$INSTALL/logs**. The word *assertion* commonly appears in core messages. Try to establish what caused the problem and contact Cisco TAC.

radclient

The Prime Access Registrar package provides a utility called **radclient** that allows RADIUS requests to be generated. Use **radclient** to test configurations and troubleshoot problems.

Cisco Prime Access Registrar Replication

For more information about using Prime Access Registrar replication, see Chapter 12, “Using Replication.”

Checking Prime Access Registrar Server Health Status

To check the server’s health, use the **aregcmd** command **status**. The following issues decrement the server’s health:

- Multiple occurances of Access-Request rejection

Note One of the parameters in the calculation of the Prime Access Registrar server’s health is the percentage of responses to Access-Accepts that are rejections. In a healthy environment, the rejection percentage will be fairly low. An extremely high percentage of rejections could be an indication of a Denial of Service attack.

- Configuration errors

- Running out of memory
- Errors reading from the network
- Dropping packets that cannot be read (because the server ran out of memory)
- Errors writing to the network.

Prime Access Registrar logs all of these conditions. Sending multiple successful responses to any packet, increments the server's health.