Managing Cisco IPICS Processes

When you start the Cisco IPICS server, the server software automatically starts the following components:

- Tomcat service
- Informix database
- Cisco Security Agent

There may be circumstances in which you need to manually stop or start one of these components. To do so, you must log in to the Cisco IPICS server and perform command line interface (CLI) procedures in a Cisco Linux terminal window.

This chapter also includes the procedure that you need to follow to change the root user password on the Cisco IPICS server.

Tip This chapter describes how to perform procedures directly on the Cisco IPICS server by using a terminal window from the Cisco Linux desktop. You can also perform these procedures by connecting to the Cisco IPICS server remotely by using the SSH Tectia Client.

This chapter includes the following sections:

Performing Tomcat Service Procedures

The Tomcat service is the main Cisco IPICS process and contains all of the Cisco IPICS web applications. For the Cisco IPICS server software to function, the Tomcat service must run continuously.

Cisco IPICS provides a cron job that checks the status of the Tomcat service every 60 seconds and can restart the service automatically, if the Tomcat service stops. The automatic restart occurs based on a setting in the tomcatcron file, which is located in the **/opt/cisco/ipics/tomcat** directory.

When the RESTART_TOMCAT_ON_ERROR value in the tomcatcron file is set to true, the cron job attempts to restart the Tomcat service if the service stops. If this value is set to false, the cron job continues to check the Tomcat service status, but does not attempt to restart the service.

If the cron job makes an attempt to restart the service, the CRON_ERROR_COUNT value in the tomcatcron file changes from 0 to 1. If the restart attempt is unsuccessful, the cron job continues to attempt the restart until the CRON_ERROR_COUNT reaches 3.

After the third attempt, the cron job continues to monitor the Tomcat service status, but does not make further attempts to restart the service. If you start the Tomcat service manually, the cron job will recognize that the Tomcat service has started again and will reset the CRON_ERROR_COUNT to 0.

If you need to perform a maintenance function that requires stopping the Tomcat service, you must adjust the RESTART_TOMCAT_ON_ERROR value. To stop the Tomcat service and adjust the file, see the "Stopping the Tomcat Service" section on page 1-3

This section includes the following topics related to the Tomcat service:

Checking the Status of the Tomcat Service

If the Tomcat service stops and the cron job cannot restart it, none of the features in Cisco IPICS can operate. In this event, users would be unable reach the Cisco IPICS Administration Console.

If you cannot access Cisco IPICS with your browser, check the status of the Tomcat service by performing the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#ps -ef | grep tomcat**

If the Tomcat service is running properly, the grep command returns a process similar to the following example:

```
root      5270     1  2 11:30 ?        00:01:33
/opt/cisco/ipics/jre/bin/java -server -Xms64m -Xmx256m -DMP_DATA=
-Djava.security.auth.login.config==/opt/cisco/ipics/tomcat/security/
.java.login.config
-Djava.security.auth.policy==/opt/cisco/ipics/tomcat/security/
.java.policy -Djava.util.logging.manager=org.apache.juli.
```

If the Tomcat service is not running, the response to the grep command is similar to the following example:

```
root      5773  5723  0 12:29 pts/1    00:00:00 grep tomcat
```

If the grep command shows that the Tomcat service is not running, you can start it manually by using a CLI procedure. For more information, see "Starting the Tomcat Service" section on page 1-5.

Stopping the Tomcat Service

If you perform a procedure such as database maintenance, you may have to stop the Tomcat service to avoid user logins. However, because of the cron job that restarts Tomcat automatically, you must first temporarily stop the cron job.

To stop the Tomcat service, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Stop the automated restart routine in the cron job by performing the following procedure:

a. To locate the tomcatcron file so that you can halt the automatic restart process, navigate to the /opt/cisco/ipics/tomcat directory by entering the following command:

[root] **#cd /opt/cisco/ipics/tomcat**

b. To edit the tomcatcron file, enter the following command:

[root] **#vi tomcatcron**

Cisco Linux opens the file for editing. The RESTART_TOMCAT_ON_ERROR setting specifies true (activated) by default.

c. To deactivate the restart routine, you must edit the RESTART_TOMCAT_ON_ERROR value and change the setting to false. You can adjust the setting by using the **Arrow** keys to move your cursor over the word, true. Then, press x to delete each letter.

d. To enter characters, press **I** to insert and then enter characters. Press **Esc** when you have finished entering characters.

e. When you have finished editing, enter **:wq!** and then press **Enter** to save the file.

Note Make sure that you repeat Steps a through e to set the RESTART_TOMCAT_ON_ERROR value to true again after you complete your maintenance and manually restart the Tomcat service.

Step 4 To stop the Tomcat service, enter the following command at the prompt:

[root] **#/etc/init.d/ipics_tomcat stop**

If the Tomcat service stops successfully, Cisco Linux displays the message, [OK].

If the Tomcat service does not successfully stop, Cisco Linux displays an error message. If you cannot stop the Tomcat service, continue to Step 5.

Step 5 If the Tomcat service fails to stop, you can kill the processes that are running by performing the following procedure:

a. To check what Tomcat processes are still running, enter the following command:

[root] **#ps -ef | grep tomcat**

The grep command returns information about the Tomcat processes that are still running. Note the Process IDs, which display in the second column of the grep results.

b. To stop any Tomcat processes that are still running, enter the following command:

[root] **#kill -9 *<process ID>***

c. Repeat Step b for every Tomcat process that is running.

d. Delete the tomcat.pid file by entering the following command:

[root] **#rm -rf /var/run/tomcat.pid**

e. Remove the /var/lock/subsys/ipics_tomcat directory by entering the following command:

[root] **#rm -rf /var/lock/subsys/ipics_tomcat**

After completing this procedure, you can safely start the Tomcat service again. For more information, see the "Starting the Tomcat Service" section on page 1-5.

Starting the Tomcat Service

Cisco IPICS starts the Tomcat service as part of the initial start-up process. A cron job regularly checks the Tomcat service status and restarts the service if the Tomcat service stops.

However, if the cron job fails to start the Tomcat service successfully or if you stop the service, you can also start the Tomcat service manually.

To manually start the Tomcat service, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ipics_tomcat start**

If you successfully started the Tomcat service Cisco Linux displays the message, [OK].

Note There may be a delay of a few minutes before users can access the Administration Console after the Tomcat service starts.

Step 4 Edit the tomcatcron file to reactivate the automated restart routine by adjusting the RESTART_TOMCAT_ON_ERROR setting to true. To adjust this setting, use the procedure in Step 3 in the "Stopping the Tomcat Service" section on page 1-3.

If the Tomcat service does not successfully start, check the catalina.out file (or catalina.*x-x-x*.log, where *x-x-x* is the date on which the file was created), which is located in the following directory:

/opt/cisco/ipics/tomcat/versions/5.5.9/logs

If you cannot resolve the problem with the information in the log files, contact Cisco Support.

Restarting the Tomcat Service

If you need to restart the Tomcat service when it is already running, you can use the restart command, which stops the Tomcat service and then starts it again. This procedure is helpful for circumstances such as activating the ops view feature after uploading and applying the license.

When you restart the Tomcat service, users are automatically logged out of the Administration Console and must log back in again.

To restart the Tomcat service, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ipics_tomcat restart**

After stopping, and then again after starting, the Tomcat service, Cisco Linux displays the message, [OK].

Note There may be a delay of a few minutes before users can access the Administration Console after the Tomcat service restarts.

Performing Informix Database Procedures

In rare circumstances, you may need to stop or start the Informix database, which you can do by enter CLI commands in a Cisco Linux terminal window on the Cisco IPICS server. To check the status of the database, you can enter a CLI command or open the System Status window in the Administration Console.

This section includes the following topics:

Checking the status of the Informix Database

Cisco IPICS includes the Administration Console GUI that allows the system administrator to check the status of the Informix database. See the "The System Status Window" section on page 3-1 for more information.

However, if you cannot log in to the Cisco IPICS Administration Console through the Login window with a valid user ID and password, you can manually check the status of the Informix database.

To check the database status from a Cisco Linux terminal window, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#ps -ef | grep oninit**

If the database is running properly, the grep command returns a process similar to the following example:

```
informix  5575     1  0 Oct26 ?        00:00:50
/opt/cisco/ipics/database/current/bin/oninit -r
root      5576  5575  0 Oct26 ?        00:00:08
/opt/cisco/ipics/database/current/bin/oninit -r
root      5577  5576  0 Oct26 ?        00:00:02
/opt/cisco/ipics/database/current/bin/oninit -r
root      5578  5576  0 Oct26 ?        00:00:00
/opt/cisco/ipics/database/current/bin/oninit -r
```

```
root      5579  5576  0 Oct26 ?        00:00:01
/opt/cisco/ipics/database/current/bin/oninit -r
root      5580  5576  0 Oct26 ?        00:00:00
/opt/cisco/ipics/database/current/bin/oninit -r
root     15750 15700  0 14:12 pts/1    00:00:00 grep oninit
```

If the database is not running, the response to the grep command is similar to the following example:

```
root     15750 15700  0 14:12 pts/1    00:00:00 grep oninit
```

If the grep command indicates that the database is not running, start the database. For more information, see the "Starting the Informix Database" section on page 1-10l.

Stopping the Informix Database

Stopping the Informix database would only be necessary if you discover that the database is slowing the performance of Cisco IPICS.

Note If you are experiencing slow performance for Cisco IPICS activity, you could determine whether the database is causing this effect only by checking the amount of system resources that the database is consuming. To perform this check, use the Cisco Linux **top** command from a Cisco Linux terminal window or an SSH Tectia Client window.

To stop the Informix database, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ipics_db stop**

If the database stops successfully, Cisco Linux displays the message, [OK].

If the database does not successfully stop, Cisco Linux displays an error message. If you cannot stop the database, continue to Step 4.

Step 4 If the database fails to stop, you can kill the processes that are running by performing the following procedure:

a. To check what database processes are still running, enter the following command:

[root] **#ps -ef | grep oninit**

The grep command returns information about the database process that are still running. Note the Process IDs, which display in the second column of the grep results.

b. To stop any database processes that are still running, enter the following command:

[root] **#kill -9 *<process ID>***

c. Repeat Step b for every database process that is running.

Starting the Informix Database

Cisco IPICS starts the Informix database as part of the initial start-up process. You can also start the Informix database manually, if you determine that the database has stopped for any reason. To check whether the database is running, see the "Checking the status of the Informix Database" section on page 1-8.

To manually start the Informix database from a Cisco Linux terminal window, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ipics_db start**

If you successfully started the database, Cisco Linux displays the message, [OK].

If the database does not successfully start, check the diagnostics.log file, which is located in the following directory:

/opt/cisco/ipics/database/logs

If you cannot resolve the problem with the information in the log file, contact Cisco Support.

Performing Cisco Security Agent Procedures

Cisco Security Agent (CSA) prevents the user (or an intruder) from performing actions on the Cisco IPICS server that may disable the server. There may be times where stopping CSA is necessary to perform system-level functions, to debug an issue, or to edit system files.

Note If you chose not to install CSA when you installed the Cisco IPICS server software, you can install CSA at any time by using a CLI procedure in a Cisco Linux terminal window.

If you installed CSA, there may be situations where you need to manually uninstall the software. For information about manually installing or uninstalling CSA, refer to the *Cisco IPICS Server Installation Guide*.

This section includes the following topics:

Viewing CSA Messages

If CSA denies a particular action, such as when a user or process attempts to modify or delete a protected file, the process generates a message similar to the following example:

```
Oct 15 04:02:02 [hostname] CiscoSecurityAgent[3480]: Event: The
process '/bin/cp' (as user root(0) group root(0)) attempted to access
'/var/cache/man/whatis'. The attempted access was an open. The
operation was denied.
```

You can access these messages in the following ways:

The CSA utility Messages pane

To view status messages in the CSA utility Messages pane, double-click the CSA tray icon (the red flag) to open the utility. The Messages pane displays by default.

Security Event Log in the CSA utility

To view the Security Event Log in the CSA utility, double-click the CSA tray icon (the red flag) to open the utility. Then, click **View Logs**.

Security Event Log in a text view

To view the Security Event Log in a text viewer, perform the following procedure:

Step 1 To view the contents of the log directory, open a terminal window by clicking the **Red Hat** icon. Then, choose **System Tools > Terminal**.

Step 2 Navigate to the /var/log directory on the Cisco IPICS server by entering the following command:

[root] **#cd /var/log**

Step 3 To list the files in the directory, enter the following command:

[root] **#ls -l**

The contents of the directory display. The Security Event Log file is named csalog. If the file has reached the maximum size one or more times, there will be more than one csalog file in the directory. Subsequent files are named csalog.0, csalog.1, csalog.2, and so on. The log that has the largest numeric extension is the current file.

Step 4 To view the log file, enter the following command:

[root] **#cat csalog.*x***

where *x* is the numeric extension, if applicable.

A text viewer window displays the contents of the Security Event Log.

Stopping CSA

You can temporarily stop CSA with the Cisco Security Agent utility or by issuing a command in a Cisco Linux terminal window.

This section includes the following topics:

- Stopping CSA with the CSA Utility, page 1-13
- Stopping the CSA Using a CLI Procedure, page 1-14

Stopping CSA with the CSA Utility

To stop the CSA process in the CSA utility, perform the following procedure:

Procedure

Step 1 To stop CSA, open the CSA utility by performing one of the following actions:

- Click the **Red Hat** icon from the Cisco Linux desktop and choose **Cisco Security Agent > Cisco Security Agent**
- Click the CSA tray icon (the red flag)

Step 2 To display the current security setting, click **System Security**.

Step 3 To stop CSA, drag the Security Level button to **Off**.

Step 4 Click **OK**.

Level 0 indicates that CSA is turned off. The CSA utility window closes.

Stopping the CSA Using a CLI Procedure

To stop the CSA from a Cisco Linux terminal window, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ciscosec stop**

If you successfully stop CSA, Cisco Linux displays the message, [OK].

Starting CSA

If you installed it with the Cisco IPICS server software, CSA starts automatically when the Cisco IPICS server boots up. If you stop CSA or if CSA stops on its own for any reason, you can restart it in the CSA utility or by performing a CLI procedure from a Cisco Linux terminal window.

This section includes the following topics:

- Starting the CSA with the CSA Utility, page 1-14
- Starting CSA Using a CLI Procedure, page 1-15

Starting the CSA with the CSA Utility

To start the CSA process in the Cisco Security Agent utility, perform the following procedure:

Procedure

Step 1 To start the Cisco Security Agent utility program, perform one of the following actions:

- Click the **Red Hat** icon from the Cisco Linux desktop and choose **Cisco Security Agent > Cisco Security Agent**.
- Double-click the CSA tray icon (the red flag) to open the utility.

The Cisco Security Agent utility displays.

Step 2 To display the current security setting, click **System Security**.

Step 3 To start the Cisco Security Agent, drag the Security Level button to **Medium**.

Step 4 Click **OK**.

The security level changes to Medium and the CSA utility window closes.

Starting CSA Using a CLI Procedure

To start the CSA process from a Cisco Linux terminal window, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 Enter the following command at the prompt:

[root] **#/etc/init.d/ciscosec start**

If you successfully start CSA, Cisco Linux displays the message, [OK].

Changing the Cisco Linux Root Password

You can change the password for the Cisco Linux root user on a periodic basis to ensure system security. You should also change the password immediately if you suspect that it is known to an unauthorized person.

To change the Cisco Linux root user password, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server with root user privileges.

The Cisco Linux desktop displays.

Step 2 To enter a CLI command, open a Cisco Linux terminal window by clicking the **Red Hat** menu and choosing **System Tools > Terminal**.

A terminal window displays.

Step 3 To temporarily disable the Cisco Linux restrictions that apply to changing the root password, enter the following command:

[root] **#sh /root/.security/unimmunize.sh**

Step 4 To create a new root password, enter the following command:

[root] **#passwd**

Cisco Linux displays a message that it is changing the password for the root user.

Step 5 At the New Password prompt, enter a new root password and press **Enter**.

When you enter your password, no characters display.

Note Your new password must be a minimum of six characters and cannot be based on a dictionary word.

Step 6 At the Retype New Password prompt, enter the new password again and press **Enter**.

Step 7 If your password is valid and you retyped it correctly, the following message displays:

```
passwd: all authentication tokens updated successfully.
```

Step 8 To reenable the Cisco Linux restrictions that apply to changing the root password, enter the following command:

[root] #**sh /root/.security/immunize.sh**

Step 9 To close the terminal window, click **X**.

The Linux desktop displays.