Additional Administrative Tasks

This section describes administrative tasks that are not done through the WAE UI.

Starting and Stopping Services Using the CLI

Note To manage (start, stop, enable monitoring, or run services at system boot) WAE services using the WAE UI, see Managing and Configuring Services.

To determine which services are running, enter the following command:

```
service --status-all | grep -i wae
```

The installation process automatically starts the `wae-web-server`, `wae-ni`, and all System services (`wae-svcs-*`).

Note To change the behavior of the `wae-web-server` service upon restarting it, you can edit the `/opt/cariden/etc/sysconfig/wae-web-server.cfg` file. For information, see the *Cisco WAE Server Installation Guide*.

You can start, restart, and obtain the status of all Automation and WAE services using the following formats, respectively.

```
service <service_name> start
service <service_name> restart
service <service_name> status
```

You can start, stop, and restart Automation and WAE services from the Statistics > Processes page, as well as enable or disable the monitoring of them. The one exception is `wae-web-server`, which can only be stopped or restarted from the CLI.

You cannot shut down a System service since these are required for the Statistics UI to properly function.

Changing Encrypted Passwords

You can update the associated configuration files for the following encrypted passwords:

- Northbound RESTful API user password
- Cisco Network Service Orchestrator (NSO) Network Configuration (NetConf) API access
- Internal system password
- SSH password for the upload of plan files to the target host

Step 1 Enter the following command:

```
wae-automation-deploy -update passwords
```

Step 2 When prompted, enter the following information:

- WAE user name—This should be the same username that was designated during software installation on the primary (local) server.
- Planning host—IP address of the primary (local) server.
- Automation host—IP address of the secondary server.
- Root user (cariden is the default root user) password for the primary server

Step 3 When prompted for each encrypted password, do one of the following:

- To change the password, enter a new password and press the **Return** key.
- To make no changes and keep the existing password, leave prompt blank and press the **Return** key.

Installing an SSL Web Certificate

As an administrator with root privileges, you can use the `install_web_certificate` tool to install certificates for WAE UI and WAE application use.

Before You Begin

Obtain the proper SSL certificate from certificate authority (CA) and have your private key file.

Step 1 Confirm that the WAE web service is running:

```
service wae-web-server status
```

Step 2 Enter the following command:

```
wae_install_web_certificate -k <private_key_file> -c <signed_certificate_file> -a
<ca_authority_file>
```

For example:

```
wae_install_web_certificate -k /path/to/172.28.101.204.web.key -c
/path/to/172.28.101.204.web.crt -a /path/to/172.28.101.204.ca.crt
```

Note

- You must include -key and - cert options when running this tool. To view help information, enter `wae_install_web_certificate` command with no options.
- Backup certificate files are created in $WAE_ROOT/etc/cert. To view tasks being performed and what files are affected run the command with the -verbose option.

Step 3 When prompted to restart services, enter `y`.

Step 4 Launch WAE UI.

Viewing Temporary Files

Temporary files can be found in the following directories:

- If $WAE_ROOT is set as a directory:
  $WAE_ROOT/data/<product_component>/tmp/

  For example, /opt/cariden/data/wae-ni/tmp
- If $WAE_ROOT is not set, and $TMPDIR is set:

  $TMPDIR/<product_component>/tmp/

  For example, /opt/tmpdir/wae-ni/tmp/
- If $WAE_ROOT and $TMPDIR are not set:

  /tmp/<product_component>/tmp/

  For example, /tmp/wae-ni/tmp/

Limiting Application Server Access to Specific IP Addresses

Step 1 Stop the Tomcat application server.

Step 2 Edit the $CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/conf/server.xml file by adding the following line:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="127.0.0.1,
[tomcat_IP],[approved_IP_addresses]"/>
```

where *approved_IP_addresses* is the list of IP addresses that can access the application server and *tomcat_IP* is the Tomcat IP address of the listening interface.

Step 3 Start the Tomcat application server. Only the clients from the approved IP address list can access the application.