To troubleshoot a configuration update, see the following sections:

Contents

Config update failed

Symptom:

The Device configuration update fails.

Solution:

To resolve this problem, follow these steps:

Step 1 Check the following on the Cisco Configuration Engine:

a. Make sure that the Event ID and Config ID match with what is defined on the device.

b. Make sure that the object status for the device in Cisco Configuration Engine is green. Green indicates that the Cisco Configuration Engine and the device are connected.

To verify that TibGate is up and running, enter the following command:

/etc/rc.d/init.d/EvtGateway status

/etc/rc.d/init.d/EvtGatewayCrypto status

Note If encryption is enabled, the TibGate ports begin with even numbers that begin from 11014. If encryption is not enabled, the TibGate ports begin with odd numbers that begin from 11013. Each TibGate port can support a maximum of 500 devices. You specify the number of the TibGates during the Cisco Configuration Engine Setup program. Make sure that the number of devices on each TibGate port does not exceed the maximum. For details, see the "Scalability Among Event Gateway Ports" chapter in the Cisco Configuration Engine Installation and Configuration Guide, 3.5.

d. If the authentication feature is enabled in the Cisco Configuration Engine, make sure that the device password (cns password <password string>) that is defined in the Cisco Configuration Engine user interface, matches with what is defined on the device. Otherwise, use the resync device command to reset the CNS password.

To use the resync command from the Cisco Configuration Engine user interface, do the following:

a. Go to Devices > Resync Device. The Resync Device page appears with a Groups list.

b. From the Groups list, choose the group that contains the device you want to resynchronize. Then click the icon for the device.

c. In the confirmation window, click Ok.

e. Make sure that the downloading configuration semantics and syntax for the device are correct.

If the device in the Cisco Configuration Engine was initially set as None, then deleted, and then re-created as an agent-enabled device, you must rename the Config ID and Event ID on both the device and the Cisco Configuration Engine user interface.

g. If during the Cisco Configuration Engine setup, a port other than the default port 80 is configured for HTTP, make sure that the same port number is also configured on the device.

Step 2

Check the following on the device:

a. Make sure that the following Event ID string is defined:cns id string <id string> cns id string <id string> event The default value of the <id string> is the hostname of the device. This ID must be the same as the Config ID defined in the Cisco Configuration Engine host.

b. To verify that the Cisco Configuration Engine hostname or IP address is specified to receive events, enter the following command:cns event <configengine hostname> 11011 keepalive 30 10

Note Make sure that the TibGate port of this device is correct. The TibGate port must match the port that is defined in the Cisco Configuration Engine.

c. If the authentication feature is enabled in the Cisco Configuration Engine, make sure that the device password (cns password <password string>) matches what is defined in the Cisco Configuration Engine user interface.

Note You cannot see the password setting after you configure it on the router, nor can you edit the password in Cisco Configuration Engine. Therefore, you must reset the password. To reset the password, use the Resync Device feature in the Cisco Configuration Engine.

d. During the Cisco Configuration Engine setup, if a port other than the default port 80 is configured for HTTP, make sure that the same port number is also configured on the device. To configure the http port on the device, enter the following command:cns config partial <CE hostname> <http port>

Step 3 If you have tried all the preceding steps and the device configuration update still fails, enable the debugging tools.

? In the Cisco Configuration Engine host, do the following:

? To start event listener, enter the following commands:cd $CISCO_CE_INSTALL_ROOT/CSCOcnsie/tools./cns-listen "cisco.>"

? Check the cfgsrv log file. This file is located at: /var/log/CNSCE/cfgsrv/cfgsrv.log.

? In the device, use the debug cns config all command to enable debugging. Analyze the output to verify that the device is set up correctly with proper connectivity.

Step 4 Rerun the scenario, check the event traffic and the information from the device, capture the data, and then contact the Cisco TAC for assistance.

Config job stuck or The configuration update is stuck in queue after data migration.

Symptom :

The configuration update is stuck in queue after data migration. Solution :

After data migration from release 2.0 to 3.5, the OpenLDAP schema is transferred to a new host. To reuse the existing OpenLDAP schema for the new host, make sure that the country code and the company code information on the new host matches what is defined on the old host.

Note The country code and the company code in the OpenLDAP schema are case sensitive.

Step 1 To reinitialize the system, enter the following command:/opt/ConfigEngine/CSCOcnsie/reinitialize

Step 2 To run data migration again, enter the following command:/opt/ConfigEngine/CSCOcnsie/bin/datamigrate

Step 3 To run the Setup program again, enter the following command:/opt/ConfigEngine/CSCOcnsie/setup

Note Make sure that you run the Setup program in bash shell. If the shell is not in bash, press ctrl-c to exit. Configure your shell in bash, and then rerun the Setup program.

Step 4 When entering the Setup parameters, make sure that the country code and the company code information for the new host matches what is defined on the old host.

For detailed information about the parameters in the Setup program, see the Cisco Configuration Engine Administration Guide.

The configuration update is stuck in the queue after data backup and restore.

Problem :

The configuration update is stuck in the queue after data backup and restore. Solution :

When you back up data and restore it, the OpenLDAP schema is transferred to a new host. To reuse the existing OpenLDAP schema for the new host, make sure that the country code and the company code information on the new host matches what is defined on the old host.

Note The country code and the company code in the OpenLDAP schema are case sensitive.

Step 1 To reinitialize the system, enter the following command:/opt/ConfigEngine/CSCOcnsie/reinitialize

Step 2 To run data restore again, enter the following command:/opt/ConfigEngine/CSCOcnsie/bin/datarestore

Step 3 To run the Setup program again, enter the following command:/opt/ConfigEngine/CSCOcnsie/setup

Note Make sure that you run the Setup program in bash shell. If the shell is not in bash, press ctrl-c to exit. Configure your shell in bash, and then rerun the Setup program.

Step 4 When entering the Setup parameters, make sure that the country code and the company code information for the new host matches what is defined on the old host.

For detailed information about the parameters in the Setup program, see the Cisco Configuration Engine Administration Guide.

CNS-Enabled Device Unable to Connect with CCE

Problem: A device is created in the Cisco Configuration Engine user interface but the device indicator displays a red status.

Possible Cause: The red status indicates that the device is unable to connect with Cisco Configuration Engine or it is still trying to connect. A connection delay might occur due to the device setting of the backoff timer. After the time has expired, the indicator does not turn to green, follow the steps given below.

Solution: To resolve this problem, follow these steps:

1. Make sure that the Event ID and Config ID match with what is defined on the device.

```
Do the following from the Cisco Configuration Engine user interface:
```

a. Choose **Devices > Edit Device**. The Edit Device page appears with a Groups list.

b. From the Groups list, choose the group that contains the device, then click the icon for the device.

c. From the left pane, choose Edit Information. The Enter Device Information page appears.

d. Click Next. The Select Group Membership page appears.

e. Click Next. The Device IDs page appears.

f. Verify that the Event ID and Config IP match with what is defined on the router.

2. Make sure that the device type is Agent Enabled Device. From the Cisco Configuration Engine user interface, do the following:

a. Choose **Devices>Edit Device**. The Edit Device page appears with a Groups list.

b. From the Groups list, choose the group that contains the device. Then click the icon for the device.

c. From the left pane, choose Edit Information. The Enter Device Information page appears.

d .Verify that the device type is Agent Enabled Device.

3. Ping or telnet to the device to verify that the device is reachable from Cisco Configuration Engine.

4. From the Cisco Configuration Engine server, make sure that TibGate, httpd, and the Java process are up.

- To verify that all TibGates are up, enter the following command:

```
/etc/rc.d/init.d/EvtGateway status
  /etc/rc.d/init.d/EvtGateway status
```

Note: For information about TibGate event gateway ports, see the ?Scalability Among Event Gateway Ports? chapter in the Cisco Configuration Engine Installation and Configuration Guide, 3.5.

- To verify that httpd is up, enter the following command:

```
'httpd status
```

- To verify that the Java process is up, enter the following command:

```
ps ?ef | grep ?i java | grep ConfigEngine'
```

5. Check the following on the device:

a. Make sure that the following Event ID string is defined:

```
cns id string <id string>
cns id string <id string> event
```

The default value of the <id string> is the hostname of the device. This ID must be the same as the Config ID defined in the Cisco Configuration Engine host.

b. To verify that the Cisco Configuration Engine hostname or IP address is specified to receive the events, enter the following command:

```
'cns event <configengine hostname or ip address> keepalive 30 10
```

c. To verify that the Cisco Configuration Engine hostname or IP address is reachable from the device, enter the following command:

```
ping <configengine hostname or ip address>
```

d. If you are unable to reach the device through the ping command, use the **ip host** command to configure the device:

```
ip host <hostname> <ip address>
   ip host <hostname.domainame> <ip address>
```

e.(Optional) To resolve hostnames, set up the DNS on the device by entering the following command:

```
ip name-server <ip address of DNS>
```

6. If the device status changes from green to red after Cisco Configuration Engine set up, follow the steps in ?Device Status? section.

CNS-Enabled Device Configuration Update Failed

Problem: The Device configuration update fails.

Possible Cause: This problem can occur for one of the following reasons:

- Invalid commands in the configuration template
- Device is not online (RED)

Solution: To resolve this problem, follow these steps:

If the device appears RED (offline), go to Step 2 and 3 to make the device GREEN (online) before proceeding with step 1.

a. In the Cisco Configuration Engine host, start the event listener and enter the following commands:

```
cd $CISCO_CE_INSTALL_ROOT/CSCOcnsie/tools
    ./cns-listen ?cisco.>?
```

Check the cfgsrv log file. This file is located at: /var/log/CNSCE/cfgsrv/cfgsrv.log. In the device, use the **debug cns all** command to enable debugging. If debug messages displays the CNS_INVALID_CLI_CMD as shown below, the config template might contain invalid commands. Apply those commands one by one on the router to find which command failed and remove or fix them from the template.

```
85E1E440: 7572653E 3C696465 6E746966 6965723E ure><identifier>
85E1E450: 31323635 38333937 32393339 32313C2F 12658397293921</
85E1E460: 6964656E 74696669 65723E3C 636F6E66 identifier><conf
85E1E470: 69672D69 643E4643 48313333 39543032 ig-id>myDevice
85E1E480: 383C2F63 6F6E6669 672D6964 3E3C6572 </config-id><er
85E1E490: 726F722D 696E666F 3E3C6C69 6E652D6E ror-info><line-n
85E1E4A0: 756D6265 723E3930 3C2F6C69 6E652D6E umber>90</line-n
85E1E4B0: 756D6265 723E3C65 72726F72 2D6D6573 umber><error-mes
85E1E4C0: 73616765 3E434E53 5F494E56 414C4944 sage>CNS_INVALID
85E1E4D0: 5F434C49 5F434D44 3C2F6572 726F722D _CLI_CMD</error-
85E1E4E0: 6D657373 6167653E 3C2F6572 726F722D message></error-
85E1E4F0: 696E666F 3E3C2F63 6F6E6669 672D6661 info></config-fa
85E1E500: 696C7572 653E ilure>
```

2. Check the following on the Cisco Configuration Engine:

a. Make sure that the Event ID and Config ID match with what is defined on the device.

b. Make sure that the object status for the device in Cisco Configuration Engine is green. Green indicates that the Cisco Configuration Engine and the device are connected.

c. To verify that TibGate is up and running, enter the following command:

```
/etc/rc.d/init.d/EvtGateway status
   /etc/rc.d/init.d/EvtGateway status
```

Note: If encryption is enabled, the TibGate ports begin with even numbers that begin from 11012. If encryption is not enabled, the TibGate ports begin with odd numbers that begin from 11011. Each TibGate port can support a maximum of 500 devices. You specify the number of the TibGates during the Cisco Configuration Engine set up program. Make sure that the number of devices on each TibGate port does not exceed the maximum.

For details, see the ?Scalability Among Event Gateway Ports? chapter in the Cisco Configuration Engine Installation and Configuration Guide, 3.5.

d. If the authentication feature is enabled in the Cisco Configuration Engine, make sure that the device password (cns password <password string>) that is defined in the Cisco Configuration Engine user interface, matches with what is defined on the device. Otherwise, use the resync device command to reset the CNS

password.

To use the resync command from the Cisco Configuration Engine user interface, do the following:

a. Go to Devices > Resync Device. The Resync Device page appears with a Groups list.

b. From the Groups list, choose the group that contains the device you want to resynchronize. Then click the icon for the device.

c. In the confirmation window, click **Ok**.

e. Make sure that the downloading configuration semantics and syntax for the device are correct.

f. If the device in the Cisco Configuration Engine was initially set as **None**, then deleted, and then re-created as an agent-enabled device, you must rename the Config ID and Event ID on both the device and the Cisco Configuration Engine user interface.

g. During the Cisco Configuration Engine set up, if a port other than the default port 80 is configured for HTTP, make sure that the same port number is also configured on the device.

3. Check the following on the device:

a. Make sure that the following Event ID string is defined:

```
cns id string <id string>
cns id string <id string> event
```

The default value of the <id string> is the hostname of the device. This ID must be the same as the Config ID defined in the Cisco Configuration Engine host.

b. To verify that the Cisco Configuration Engine hostname or IP address is specified to receive events, enter the following command:

```
cns event <configengine hostname or ip address> keepalive 30 10
```

Note: Make sure that the TibGate port of this device is correct. The TibGate port must match the port that is defined in the Cisco Configuration Engine.

c. If the authentication feature is enabled in the Cisco Configuration Engine, make sure that the device password (cns password <password string>) matches what is defined in the Cisco Configuration Engine user interface.

Note: You cannot see the password setting after you configure it on the router, nor can you edit the password in Cisco Configuration Engine. Therefore, you must reset the password. To reset the password, use the Resync Device feature in the Cisco Configuration Engine.

d. During the Cisco Configuration Engine set up, if a port other than the default port 80 is configured for HTTP, make sure that the same port number is also configured on the device. To configure the http port on the device, enter the following command:

```
cns config partial <CE hostname> <http port>
```

4. If you have tried all the preceding steps and the device configuration update still fails, enable the debugging tools.

- In the Cisco Configuration Engine host, start the event listener by enter the following commands:

```
cd $CISCO_CE_INSTALL_ROOT/CSCOcnsie/tools
   ./cns-listen ?cisco.>?
```

- Check the cfgsrv log file. This file is located at: /var/log/CNSCE/cfgsrv/cfgsrv.log.

- In the device, use the debug **cns config all** command to enable debugging. Analyze the output to verify that the device is set up correctly with proper connectivity.

5. Re-run the scenario, check the event traffic and the information from the device, capture the data, and then contact the Cisco TAC for assistance.

Configuration Update Stuck in Queue After Data Migration

Problem: The configuration update is stuck in queue after data migration.

Possible Cause: This problem can occur if you did not enter the correct country code and company code information during the set up program.

Solution: After data migration from release 3.0 to 3.5, the OpenLDAP schema is transferred to a new host. To reuse the existing OpenLDAP schema for the new host, make sure that the country code and the company code information on the new host matches with what is defined on the old host. Follow these steps:

1. To reinitialize the system, enter the following command:

```
/opt/ConfigEngine/CSCOcnsie/reinitialize
```

2. To run data migration again, enter the following command:

```
/opt/ConfigEngine/CSCOcnsie/bin/datamigrate
```

3. To run the set up program again, enter the following command:

```
opt/ConfigEngine/CSCOcnsie/setup
```

Note: Make sure that you run the set up program in bash shell. If the shell is not in bash, press ctrl-c to exit. Configure your shell in bash, and then re-run the set up program.

4. When entering the set up parameters, make sure that the country code and the company code information for the new host matches with what is defined on the old host.

Note: The country code and the company code in the OpenLDAP schema are case sensitive.

For detailed information about the parameters in the set up program, see the Cisco Configuration Engine Administration Guide.

```
Example:

Choose operational mode of system. 0=internal directory mode,
1=external directory mode. [0]
Enter country code: us
Enter company code: cisco
```

Configuration Update Stuck in Queue After Data Backup and Restore

Problem: The configuration update is stuck in the queue after data backup and restore.

Possible Cause: This problem can occur if you did not enter the correct country code and company code information during the set up program.

'**Solution**: When you back up data and restore it, the OpenLDAP schema is transferred to a new host. To re-use the existing OpenLDAP schema for the new host, make sure that the country code and the company code information on the new host matches with what is defined on the old host. Follow these steps:

1. To reinitialize the system, enter the following command:

/opt/ConfigEngine/CSCOcnsie/reinitialize

2. To run data restore again, enter the following command:

/opt/ConfigEngine/CSCOcnsie/bin/datarestore

3. To run the set up program again, enter the following command:

/opt/ConfigEngine/CSCOcnsie/setup

Note: Make sure that you run the set up program in bash shell. If the shell is not in bash, press ctrl-c to exit. Configure your shell in bash, and then re-run the set up program.

4. When entering the set up parameters, make sure that the country code and the company code information for the new host matches with what is defined on the old host.

Note: The country code and the company code in the OpenLDAP schema are case sensitive.

For detailed information about the parameters in the set up program, see the Cisco Configuration Engine Administration Guide.

```
Example

Choose operational mode of system. 0=internal directory mode,
1=external directory mode. [0]
Enter country code: us
Enter company code: cisco
```

Config job failed with parser error

Problem :

The configuration update job failed with ?%CNS-3-XML_SEMANTIC: CNS_FW_XML_PARSE_ERROR?

Solution : To resolve this problem, follow these steps:

Step 1 Identify which CLI in the configuration job template caused the error

Step 2 Type that CLI directly on the device config terminal and see whether the CLI is support.

Step 3 If the CLI results an error, it means the CLI is not supported or has problem in the IOS version that the customer is using, report the problem to cns-ios-sw mailer. If the CLI has no problem in executing on the device, report to cs-ce mailer for further debug.

Config job fails for commands like "show run", "tclsh" etc

Problem :

The configuration update job fails for execution commands like "show run", "tclsh" etc and respond back with error messages like "CNS_FW_XML_PARSE_ERROR?, "AUTHORIZATION_FAILURE" etc. The debug of CNS will show errors like "Received malformed or errant xml".

Solution : To commands like "show run", "tclsh" are execution commands in the device and are not configurations. These commands cannot be directly executed on the configuration terminal and so should not be pushed as part of configuration update which acts only on configuration. Verify the execution of commands used in configuration update on the configuration terminal of the device.