CHAPTER 1

Overview of Cisco Unity Connection 9.x Troubleshooting

The *Troubleshooting Guide for Cisco Unity Connection* helps you resolve problems that you might encounter with Connection. If your Connection system is exhibiting a symptom that is documented in this troubleshooting guide, perform the recommended troubleshooting procedures. However, if the symptom is not documented in this troubleshooting guide, or if the recommended troubleshooting does not resolve the problem, do the following procedure to determine whether the problem might be caused by SELinux Security policies. (SELinux replaced Cisco Security Agent(CSA) on Connection servers.)

To Troubleshoot Symptoms that Cannot Be Resolved by Documented Troubleshooting Procedures

Step 1 To check the status of SELinux on Connection server, run the Command Line Interface (CLI) command **utils os secure status**.

Step 2 If SELinux is in Enforcing mode, run the CLI command **utils os secure permissive** to put the Connection server in Permissive mode. For more information on the CLI command **utils os secure permissive**, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 3 Try to reproduce the symptom with SELinux in permissive mode. If the symptom is reproducible, it is not caused by SELinux.

Step 4 If the symptom is not reproducible, do the following steps to gather logs before you contact Cisco TAC:

a. Create your test directory on sftp server to save the audit log diagnostic file at that location.

b. Put Connection server in Enforcing mode by running the CLI command **utils os secure enforce**.

c. Try to create the symptom again.

d. Create the audit logs diagnostic file by running the CLI command **utils create report security**. This command creates a diagnostic file “security-diagnostics.tar.gz”. Copy the diagnostic file to sftp directory created in step 4(a) by running the CLI command **file get activelog syslog/security-diagnostics.tar.gz**. For more information on the CLI command, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 5 Contact Cisco TAC.

For example, to troubleshoot the switch version failures as part of upgrade from Unity Connection 8.6 to a later version, do the following procedure.

To Troubleshoot Switch Version Failures As Part of Upgrade from Cisco Unity Connection 8.6 to a Later Version

Step 1 To check the status of SELinux on Connection server, run the Command Line Interface (CLI) command **utils os secure status**.

Step 2 If SELinux is in Enforcing mode, run the CLI command **utils os secure permissive** to put the Connection server in Permissive mode. For more information on the CLI command **utils os secure permissive**, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 3 Retry the switch version with SELinux in permissive mode. If the switch version failure is reproducible, it is not caused by SELinux.

Step 4 If the switch version failure is not reproducible, do the following steps to gather logs before you contact Cisco TAC:

a. Create your test directory on sftp server to save the audit log diagnostic file at that location.

b. Put Connection server in Enforcing mode by running the CLI command **utils os secure enforce**.

c. Try to create the symptom again.

d. Create the audit logs diagnostic file by running the CLI command **utils create report security**. This command creates a diagnostic file "security-diagnostics.tar.gz". Copy the diagnostic file to sftp directory created in step 4(a) by running the CLI command **file get activelog syslog/security-diagnostics.tar.gz**. For more information on the CLI command, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Step 5 Contact Cisco TAC.

To Troubleshoot Failsafe Message While Upgrading from Connection 8.6.(x)

If you are getting the failsafe message while upgrading from Connection 8.6.(x) in a cluster, put the system in the permissive mode using the CLI command **utils os secure permissive** command until the switch version process is completed. For more information on the CLI command used to put the system in permissive mode, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.