Troubleshooting Multi-Server Certificate

Cisco Unity Connection supports Multi-server Subject Alternate Name (SAN). See the following sections for information on troubleshooting problems with Multi-server certificates.

Initial Debugging and Identifying Topology Details

Initial Debugging

- Identify the hostname of both the publisher and subscriber nodes in the Unity Connection cluster.
- Identify the node from which the CSR was generated and pushed.
- Identify the node from which the certificate was uploaded.
- Ensure that the Cisco Tomcat and Platform Administrative Web Service (PAWS) are running.

Note You can use the utils service list CLI command to list the running services.

Collecting Log Files

The logs can be collected by the Real-Time Monitoring Tool (RTMT) or the Command Line Interface. For detailed instructions, see the "Traces and Logs" chapter of the *Cisco Unified Real-Time Monitoring Tool Administration Guide*, available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

CLI commands to List and Get Log Files

- CLI command to list the log file is file list<file name>
- CLI command to get the log file is file get<file name>

Required Log Files

There are two log files that needs to be collected for analyzing issues with Multi-server Certificate.

- Cisco Tomcat.
- Connection Branch Sync Service.

CLI Commands examples

Below are the CLI command examples to list and collect the log files.

- CLI command to list the log files:
  - file list activelog cuc/diag_Tomcat*
  - file list activelog cuc/diag_CUCE_Sync*
- CLI command to collect the log file:
  - file get activelog cuc/diag_Tomcat_00000001.uc
  - file get activelog cuc/diag_CUCE_Sync00000001.uc

After analyzing the log files, if you cannot resolve the problem, contact Cisco TAC.