Troubleshoot CUCM Cluster Backup Failure Due to Expired Certificates

Contents

Issue

CUCM cluster backups using the Disaster Recovery System (DRS) are failing. During troubleshooting of the backup failures, certificate exceptions were encountered when attempting to access IMP nodes from the CUCM Publisher. The certificate validation revealed that multiple certificates within the cluster had expired, including Tomcat trust certificates for the IMP Publisher and IMP Subscriber nodes. On the IMP Publisher, the cup, cup-xmpp, and tomcat certificates were found to be expired, with the tomcat certificate appearing as an older multi-server certificate from the CUCM Publisher.

Environment

- Cisco Unified Communications Manager (CUCM) cluster deployment
- Cisco Unified IM and Presence (IMP) Publisher and Subscriber nodes
- Disaster Recovery System (DRS) configured for cluster backups
- SFTP server configured for backup storage
- Multiple expired certificates affecting cluster communication

Resolution

To resolve the CUCM cluster backup failures caused by expired certificates, review these steps to renew the necessary certificates and restart required services:

Step 1: Renew Tomcat Certificates and IPsec Certificates on All Cluster Nodes

Renew the Tomcat certificate on each node within the cluster. You can choose either individual self-signed certificates per node or generate a multi-server tomcat certificate from the CUCM Publisher and deploy to

all nodes.

1. Navigate to **OS Administration > Security > Certificate Management** on each node to renew the Tomcat certificates. Renew the IPsec Certificates on each node within the cluster.

Step 2: Renew CUP and CUP-XMPP Certificates

After completing the Tomcat certificate renewal on all nodes, proceed to renew the cup and cup-xmpp certificates on the affected IMP nodes.

1. Navigate to **Cisco Unified IM and Presence Serviceability > Security > Certificate Management** to renew these certificates.

Step 3: Restart Required Services

Restart the services indicated and required by each node after the certificate updates are completed. The system displays which services must be restarted after certificate renewal.

Step 4: Verify DRF Services Status

Confirm the DRF Master service is running on the CUCM Publisher and DRF local services are running on all nodes in the cluster.

1. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services** to verify and start the DRF services:

- DRF Master must be running on the CUCM Publisher
- DRF Local must be running on all cluster nodes

Step 5: Test Manual Backup and Collect Logs

After completing the certificate renewal and service restarts, test the manual backup functionality and collect RTMT logs for analysis:

1. Navigate to **Cisco Unified CM Administration > System > Backup and Restore > Manual Backup** to initiate a test backup. Collect these logs using Real-Time Monitoring Tool (RTMT):

- DRF Master logs from the CUCM Publisher
- DRF Local logs from all nodes in the cluster

Cause

The CUCM cluster backup failures were caused by expired certificates within the cluster environment. Specifically, the Tomcat trust certificates for the IMP Publisher and IMP Subscriber nodes had expired, along with the cup, cup-xmpp, and tomcat certificates on the IMP Publisher. The expired certificates prevented proper SSL/TLS communication between cluster nodes, which is required for the Disaster Recovery System (DRS/BARS) to successfully perform cluster-wide backup operations. The tomcat certificate on the IMP Publisher was identified as an older multi-server certificate from the CUCM Publisher that had not been properly renewed.

Related Content

- Cisco Unified IM and Presence Configuration and Administration Guide
- Cisco Technical Support & Downloads