Dépannage de l'échec de la sauvegarde du cluster CUCM en raison de certificats expirés

Table des matières

Problème

Les sauvegardes de cluster CUCM à l'aide du système de reprise après sinistre (DRS) échouent. Lors du dépannage des échecs de sauvegarde, des exceptions de certificat ont été rencontrées lors de la tentative d'accès aux noeuds IMP à partir du serveur de publication CUCM. La validation du certificat a révélé que plusieurs certificats au sein du cluster avaient expiré, y compris les certificats de confiance Tomcat pour les noeuds IMP Publisher et IMP Subscriber. Sur l'éditeur IMP, les certificats cup, cup-xmpp et tomcat ont expiré, le certificat tomcat apparaissant comme un certificat multi-serveur plus ancien de l'éditeur CUCM.

Environnement

- Déploiement de clusters Cisco Unified Communications Manager (CUCM)
- Noeuds Éditeur et Abonné Cisco Unified IM and Presence (IMP)
- Système de reprise après sinistre (DRS) configuré pour les sauvegardes de cluster
- Serveur SFTP configuré pour le stockage de sauvegarde
- Plusieurs certificats expirés affectant la communication de cluster

Résolution

Pour résoudre les échecs de sauvegarde du cluster CUCM causés par des certificats expirés, passez en revue ces étapes pour renouveler les certificats nécessaires et redémarrer les services requis :

Étape 1: Renouveler les certificats Tomcat et IPsec sur tous les noeuds de cluster

Renouvelez le certificat Tomcat sur chaque noeud du cluster. Vous pouvez choisir des certificats auto-signés individuels par noeud ou générer un certificat tomcat multiserveur à partir du serveur de publication CUCM et le déployer sur tous les noeuds.

1. Accédez à OS Administration > Security > Certificate Management sur chaque noeud pour renouveler les certificats Tomcat. Renouvelez les certificats IPsec sur chaque noeud du cluster.

Étape 2: Renouveler les certificats CUP et CUP-XMPP

Après avoir terminé le renouvellement du certificat Tomcat sur tous les noeuds, continuez à renouveler les certificats cup et cup-xmpp sur les noeuds IMP affectés.

1. Accédez à Cisco Unified IM and Presence Serviceability > Security > Certificate Management pour renouveler ces certificats.

Étape 3: Redémarrer les services requis

Redémarrez les services indiqués et requis par chaque noeud une fois les mises à jour du certificat terminées. Le système affiche les services qui doivent être redémarrés après le renouvellement du certificat.

Étape 4: Vérifier l'état des services DRF

Vérifiez que le service DRF Master est en cours d'exécution sur le serveur de publication CUCM et que les services locaux DRF sont en cours d'exécution sur tous les noeuds du cluster.

1. Accédez à Cisco Unified Serviceability > Tools > Control Center - Feature Services pour vérifier et démarrer les services DRF :

- Le maître DRF doit être exécuté sur le serveur de publication CUCM
- DRF Local doit être exécuté sur tous les noeuds de cluster

Étape 5: Tester la sauvegarde manuelle et collecter les journaux

Une fois le renouvellement du certificat terminé et le service redémarré, testez la fonctionnalité de sauvegarde manuelle et collectez les journaux RTMT pour analyse :

1. Accédez à Cisco Unified CM Administration > System > Backup and Restore > Manual Backup pour lancer une sauvegarde test. Collectez ces journaux à l'aide de l'outil de surveillance en temps réel (RTMT) :

- Journaux principaux DRF du serveur de publication CUCM
- DRF Journaux locaux de tous les noeuds du cluster

Motif

Les échecs de sauvegarde du cluster CUCM ont été provoqués par des certificats expirés dans l'environnement de cluster. Plus précisément, les certificats de confiance Tomcat pour les noeuds IMP Publisher et IMP Subscriber avaient expiré, ainsi que les certificats cup, cup-xmpp et tomcat sur l'éditeur IMP. Les certificats expirés ont empêché une communication SSL/TLS correcte entre les noeuds de cluster, ce qui est nécessaire pour que le système de reprise après sinistre (DRS/BARS) puisse effectuer correctement les opérations de sauvegarde à l'échelle du cluster. Le certificat tomcat sur le serveur de publication IMP a été identifié comme un certificat multiserveur plus ancien du serveur de publication CUCM qui n'avait pas été renouvelé correctement.

Autres informations utiles

- Guide de configuration et d'administration de Cisco Unified IM and Presence
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.