Fehlerbehebung bei der CUCM-Cluster-Sicherung aufgrund abgelaufener Zertifikate

Inhalt

Problem

CUCM-Cluster-Backups mit dem Disaster Recovery System (DRS) sind fehlgeschlagen. Bei der Fehlerbehebung bei Sicherungsfehlern traten beim Zugriff auf IMP-Knoten vom CUCM Publisher Zertifikatausnahmen auf. Bei der Zertifikatsüberprüfung wurde festgestellt, dass mehrere Zertifikate im Cluster abgelaufen waren, einschließlich Tomcat-Vertrauenszertifikaten für die IMP Publisher- und IMP Subscriber-Knoten. Auf dem IMP-Publisher wurden die Zertifikate cup, cup-xmpp und tomcat als abgelaufen erkannt, und das tomcat-Zertifikat wird als älteres Multiserver-Zertifikat vom CUCM-Publisher angezeigt.

Umwelt

- Cisco Unified Communications Manager (CUCM) Cluster-Bereitstellung
- Cisco Unified IM and Presence (IMP) Publisher- und Subscriber-Knoten
- Für Cluster-Backups konfiguriertes Disaster Recovery System (DRS)
- SFTP-Server für Backup-Speicher konfiguriert
- Mehrere abgelaufene Zertifikate, die die Clusterkommunikation beeinflussen

Auflösung

Um die durch abgelaufene Zertifikate verursachten CUCM-Cluster-Sicherungsfehler zu beheben, überprüfen Sie die folgenden Schritte, um die erforderlichen Zertifikate zu erneuern und die erforderlichen Dienste neu zu starten:

Schritt 1: Erneuern von Tomcat-Zertifikaten und IPsec-Zertifikaten auf allen Cluster-Knoten

Erneuern Sie das Tomcat-Zertifikat für jeden Knoten im Cluster. Sie können entweder einzelne selbstsignierte Zertifikate pro Knoten auswählen oder ein Multi-Server-Tomcat-Zertifikat vom CUCM Publisher generieren und auf allen Knoten bereitstellen.

1. Navigieren Sie zu OS Administration > Security > Certificate Management auf jedem Knoten, um die Tomcat-Zertifikate zu erneuern. Erneuern Sie die IPsec-Zertifikate auf jedem Knoten im Cluster.

Phase 2: Verlängerung der CUP- und CUP-XMPP-Zertifikate

Nachdem Sie die Tomcat-Zertifikatserneuerung für alle Knoten abgeschlossen haben, können Sie die Cup- und Cup-xmpp-Zertifikate für die betroffenen IMP-Knoten erneuern.

1. Navigieren Sie zu Cisco Unified IM and Presence Serviceability > Security > Certificate Management, um diese Zertifikate zu erneuern.

Schritt 3: Erforderliche Dienste neu starten

Starten Sie die angegebenen und von jedem Knoten benötigten Dienste neu, nachdem die Zertifikataktualisierungen abgeschlossen sind. Das System zeigt an, welche Dienste nach der Erneuerung des Zertifikats neu gestartet werden müssen.

Schritt 4: DRF-Servicestatus überprüfen

Vergewissern Sie sich, dass der DRF-Master-Dienst auf dem CUCM Publisher ausgeführt wird und die lokalen DRF-Dienste auf allen Knoten im Cluster ausgeführt werden.

1. Navigieren Sie zu Cisco Unified Serviceability > Tools > Control Center - Feature Services, um die DRF-Services zu überprüfen und zu starten:

- DRF Master muss auf dem CUCM Publisher ausgeführt werden.
- DRF Local muss auf allen Clusterknoten ausgeführt werden.

Schritt 5: Manuelles Testen von Backup- und Collect-Protokollen

Nach Abschluss der Erneuerung des Zertifikats und nach Neustart des Services müssen Sie die manuelle Backup-Funktion testen und RTMT-Protokolle zur Analyse erfassen:

1. Navigieren Sie zu Cisco Unified CM Administration > System > Backup and Restore > Manual Backup, um eine Test-Sicherung einzuleiten. Erfassen Sie diese Protokolle mit dem Real-Time Monitoring Tool (RTMT):

- DRF-Master-Protokolle vom CUCM Publisher
- Lokale DRF-Protokolle von allen Knoten im Cluster

Ursache

Die CUCM-Cluster-Sicherungsfehler wurden durch abgelaufene Zertifikate in der Cluster-Umgebung verursacht. Insbesondere waren die Tomcat-Vertrauenszertifikate für die IMP Publisher- und IMP Subscriber-Knoten abgelaufen, zusammen mit den Cup-, Cup-xmpp- und Tomcat-Zertifikaten auf dem IMP Publisher. Die abgelaufenen Zertifikate verhinderten eine ordnungsgemäße SSL/TLS-Kommunikation zwischen den Clusterknoten, die erforderlich ist, damit das Notfallwiederherstellungssystem (DRS/BARS) clusterweite Sicherungsvorgänge erfolgreich durchführen kann. Das Tomcat-Zertifikat auf dem IMP Publisher wurde als älteres Multi-Server-Zertifikat vom CUCM Publisher identifiziert, das nicht ordnungsgemäß erneuert wurde.

Verwandte Inhalte

- Cisco Unified IM und Presence - Konfigurations- und Administrationsleitfaden
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.