Risoluzione dei problemi di backup del cluster CUCM a causa di certificati scaduti

Sommario

Problema

I backup dei cluster CUCM che utilizzano il Disaster Recovery System (DRS) non riescono. Durante la risoluzione dei problemi relativi agli errori di backup, sono state rilevate eccezioni di certificato durante il tentativo di accedere ai nodi IMP dal server di pubblicazione CUCM. La convalida del certificato ha rilevato che più certificati all'interno del cluster sono scaduti, inclusi i certificati di attendibilità Tomcat per i nodi del server di pubblicazione IMP e del Sottoscrittore IMP. In IMP Publisher i certificati Cup, cup-xmpp e tomcat sono scaduti, con il certificato tomcat visualizzato come un precedente certificato multiserver di CUCM Publisher.

Ambiente

- Distribuzione cluster Cisco Unified Communications Manager (CUCM)
- Nodi Cisco Unified IM and Presence (IMP) Publisher e Subscriber
- DRS (Disaster Recovery System) configurato per i backup del cluster
- Server SFTP configurato per lo storage di backup
- Più certificati scaduti influiscono sulla comunicazione del cluster

Risoluzione

Per risolvere gli errori di backup del cluster CUCM causati da certificati scaduti, rivedere i passaggi seguenti per rinnovare i certificati necessari e riavviare i servizi richiesti:

Passaggio 1: Rinnova certificati Tomcat e certificati IPsec in tutti i nodi del cluster

Rinnovare il certificato Tomcat in ogni nodo all'interno del cluster. È possibile scegliere singoli certificati autofirmati per nodo oppure generare un certificato di attivazione su più server da CUCM Publisher e distribuirlo a tutti i nodi.

1. Passare a Amministrazione sistema operativo > Protezione > Gestione certificati su ogni nodo per rinnovare i certificati Tomcat. Rinnovare i certificati IPSec in ogni nodo del cluster.

Passaggio 2: Rinnova certificati CUP e CUP-XMPP

Dopo aver completato il rinnovo del certificato Tomcat su tutti i nodi, procedere con il rinnovo dei certificati Cup e Cup-xmpp sui nodi IMP interessati.

1. Passare a Cisco Unified IM and Presence Serviceability > Security > Certificate Management per rinnovare questi certificati.

Passaggio 3: Riavvia servizi necessari

Riavviare i servizi indicati e richiesti da ogni nodo al termine degli aggiornamenti del certificato. Vengono visualizzati i servizi da riavviare dopo il rinnovo del certificato.

Passaggio 4: Verifica stato servizi DRF

Verificare che il servizio DRF Master sia in esecuzione nel server di pubblicazione CUCM e che i servizi locali DRF siano in esecuzione in tutti i nodi del cluster.

1. Passare a Cisco Unified Serviceability > Tools > Control Center - Feature Services per verificare e avviare i servizi DRF:

- DRF Master deve essere in esecuzione sul server di pubblicazione CUCM
- DRF Local deve essere in esecuzione su tutti i nodi cluster

Passaggio 5: Verifica backup manuale e raccolta registri

Dopo aver completato il rinnovo del certificato e riavviato il servizio, verificare la funzionalità di backup manuale e raccogliere i registri RTMT per l'analisi:

1. Passare a Cisco Unified CM Administration > System > Backup and Restore > Manual Backup per avviare un backup di test. Raccogliere questi log utilizzando lo strumento di monitoraggio in tempo reale (RTMT, Real-Time Monitoring Tool):

- Registri master DRF dal server di pubblicazione CUCM
- DRF Registri locali da tutti i nodi nel cluster

Causa

Gli errori di backup del cluster CUCM sono stati causati da certificati scaduti nell'ambiente cluster. In particolare, i certificati di attendibilità Tomcat per i nodi IMP Publisher e IMP Subscriber sono scaduti, insieme ai certificati cup, cup-xmpp e tomcat nell'editore IMP. I certificati scaduti hanno impedito la corretta comunicazione SSL/TLS tra i nodi del cluster, necessaria per consentire al sistema di ripristino di emergenza (DRS/BARS) di eseguire correttamente le operazioni di backup a livello di cluster. Il certificato tomcat nel server di pubblicazione IMP è stato identificato come un certificato multiserver precedente del server di pubblicazione CUCM che non è stato rinnovato correttamente.

Contenuto correlato

- Guida di configurazione e amministrazione di Cisco Unified IM and Presence
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).