Solucionar problemas de falha de backup de cluster do CUCM devido a certificados expirados

Contents

Problema

Os backups de cluster do CUCM usando o Sistema de recuperação de desastres (DRS) estão falhando. Durante a solução de problemas de falhas de backup, exceções de certificado foram encontradas ao tentar acessar nós IMP do Editor do CUCM. A validação do certificado revelou que vários certificados no cluster expiraram, incluindo certificados confiáveis Tomcat para os nós Editor e Assinante IMP. No editor IMP, os certificados cup, cup-xmpp e tomcat foram encontrados expirados, com o certificado tomcat aparecendo como um certificado de multiservidor mais antigo do editor CUCM.

Ambiente

- Implantação de cluster do Cisco Unified Communications Manager (CUCM)
- Nós do editor e do assinante do Cisco Unified IM and Presence (IMP)
- Sistema de recuperação de desastres (DRS) configurado para backups de cluster
- Servidor SFTP configurado para armazenamento de backup
- Vários certificados expirados que afetam a comunicação do cluster

Resolução

Para resolver as falhas de backup de cluster do CUCM causadas por certificados expirados, revise estas etapas para renovar os certificados necessários e reinicie os serviços necessários:

Passo 1: Renovar certificados Tomcat e IPsec em todos os nós do cluster

Renove o certificado Tomcat em cada nó no cluster. Você pode escolher certificados autoassinados individuais por nó ou gerar um certificado tomcat multiservidor do Editor do CUCM e implantar em todos os nós.

1. Navegue até OS Administration > Security > Certificate Management em cada nó para renovar os certificados Tomcat. Renove os Certificados IPsec em cada nó no cluster.

Passo 2: Renove os certificados CUP e CUP-XMPP

Após concluir a renovação do certificado Tomcat em todos os nós, continue a renovar os certificados cup e cup-xmpp nos nós IMP afetados.

1. Navegue até Cisco Unified IM and Presence Serviceability > Security > Certificate Management para renovar esses certificados.

Passo 3: Reiniciar Serviços Necessários

Reinicie os serviços indicados e exigidos por cada nó após a conclusão das atualizações do certificado. O sistema exibe quais serviços devem ser reiniciados após a renovação do certificado.

Passo 4: Verificar o status dos serviços DRF

Confirme se o serviço DRF Master está em execução no Editor do CUCM e se os serviços locais do DRF estão em execução em todos os nós no cluster.

1. Navegue até Cisco Unified Serviceability > Tools > Control Center - Feature Services para verificar e iniciar os serviços DRF:

- O DRF Master deve estar em execução no Editor do CUCM
- O DRF Local deve estar em execução em todos os nós do cluster

Passo 5: Teste o backup manual e os registros de coleta

Após concluir a renovação do certificado e reiniciar o serviço, teste a funcionalidade de backup manual e colete os logs RTMT para análise:

1. Navegue até Cisco Unified CM Administration > System > Backup and Restore > Manual Backup para iniciar um backup de teste. Colete esses registros usando a Real-Time Monitoring Tool (RTMT):

- Logs mestres do DRF do editor do CUCM
- Logs locais do DRF de todos os nós no cluster

Causa

As falhas de backup de cluster do CUCM foram causadas por certificados expirados no ambiente de cluster. Especificamente, os certificados confiáveis do Tomcat para os nós IMP Publisher e IMP Subscriber expiraram, juntamente com os certificados cup, cup-xmpp e tomcat no IMP Publisher. Os certificados expirados impediram a comunicação SSL/TLS adequada entre os nós do cluster, o que é necessário para que o Sistema de Recuperação de Desastres (DRS/BARS) execute com êxito operações de backup em todo o cluster. O certificado tomcat no editor IMP foi identificado como um certificado de multiservidor mais antigo do editor CUCM que não foi renovado corretamente.

Conteúdo relacionado

- Guia de configuração e administração do Cisco Unified IM and Presence
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.