Instalação unificada do conjunto de uma comunicação com exemplo de configuração CA-assinado do nome alternativo do assunto do Multi-server

Índice

Introdução

Este documento descreve como estabelecer um conjunto unificado de uma comunicação com o uso de um Certificate Authority (CA) - o nome alternativo assinado do assunto do Multi-server (SAN).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Gerente das comunicações unificadas de Cisco (CUCM)
- CUCM IM e versão 10.5 da presença

Antes que você tente esta configuração, assegure-se de que estes serviços estejam ascendentes e funcionais:

- Serviço de Web administrativo da plataforma Cisco
- Serviço Cisco Tomcat

A fim verificar estes serviços em uma interface da WEB, navegue a **Cisco unificou serviços > serviço de rede da página da utilidade > selecionam um server**. A fim verificá-los no CLI, inscreva o **comando list do serviço dos utils**.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Na versão 10.5 e mais recente CUCM, este pedido da solicitação de assinatura de certificado da confiança-loja (CSR) pode incluir o SAN e domínios alternativos.

1. Tomcat
2. CallManager da Cisco (CCM)
3. Cisco unificou o protocolo Presença-elástico da Mensagem e da presença (CUP-XMPP)
4. Server-à-server CUP-XMPP (S2S)

Émais simples obter um certificado assinado CA nesta versão. Somente um CSR é exigido ser assinado por CA um pouco do que a exigência obter um CSR de cada nó de servidor e então obter um certificado assinado CA para cada CSR e controlá-los individualmente.

Configurar

1. Registre no operating system (OS) a administração e navegue ao **> gerenciamento de certificado da Segurança > gerenciem o CSR**.

2. Selecione o Multi-**server SAN na** distribuição.

   Ele autopopulates os domínios SAN e o domínio do pai.

   Uma vez que é gerado, este indica:

   No gerenciamento certificado, o pedido SAN é gerado:

3. Você pode usar CA local ou CA externo como Verisign a fim obtê-lo assinado. Este exemplo mostra etapas de configuração para CA Server-baseado Microsoft Windows.

   Registre em https:// <windowsserveripaddress>/certsrv/

   Selecione o **pedido um certificado > avançou o pedido do certificado**.

4. Submeta o pedido CSR como mostrado aqui.

5. Uma vez que você obtém o certificado, você deve transferir arquivos pela rede o certificado de CA como a Tomcat-confiança e então transferir arquivos pela rede o certificado assinado CA como TomCat.

6. Assegure-se de que o serviço esteja reiniciado em todos os Nós na lista SAN, que inclui o nó onde é transferida arquivos pela rede. Você vê o Multi-server SAN alistado no gerenciamento certificado.

Verificar

Log em http://<fqdnofccm>:8443/ccmadmin a fim assegurar-se de que o certificado novo esteja usado.

Certificado do Multi-server SAN do CallManager

Um procedimento similar pode ser seguido para o certificado do CallManager. Neste caso, os domínios autopopulated são todos os Nós do CallManager. Se não é executado, você pode escolher mantê-lo da lista SAN ou removê-lo de lá.

Depois que você instala o certificado emitido por CA, você deve reiniciar o serviço do CallManager em todos os Nós.

Antes que você obtenha o certificado CA-assinado SAN para CUCM, assegure isso:

- O telefone IP pode confiar o serviço da verificação da confiança (TV). Isto pode ser verificado se você alcança algum serviço HTTPS do telefone. Por exemplo, se o acesso do diretório corporativo trabalha, a seguir significa que o telefone confia o serviço TV.
- Se é um conjunto seguro, assegure-se de que o cliente do certificate trust list (CTL) esteja tornado a colocar em funcionamento de modo que um arquivo novo CTL seja criado e o

conjunto é recarregado.

Troubleshooting

Estes logs devem ajudar o centro de assistência técnica da Cisco a identificar todas as edições relativas à geração do Multi-server SAN CSR e à transferência de arquivo pela rede CA-Assinar Certficate.

- Cisco unificou a plataforma de OS API
- Cisco Tomcat
- Logs de CertMgr da plataforma IPT

Em um Multi-server existente Certifcate CUCM, se o hostname do server muda, recomenda-se gerar um pedido do multi-server SAN CSR como explicado previamente a fim obter o certificado assinado por CA.