Configurar o nome alternativo do assunto do multiservidor assinado pela CA em sistemas CVOS

Contents

Introdução

Este documento descreve como configurar um cluster de sistema do Cisco Voice Operating System (CVOS) com o uso de um Nome Alternativo de Assunto (SAN) de Multiservidor assinado por Autoridade de Certificação (CA) com o modelo de arquitetura editor-assinante. O sistema CVOS abrange os sistemas CUIC, Finesse, Livedata e IdS no ambiente UCCE.

Contribuição de Venu Gopal Sane, Ritesh Desai Engenheiro do Cisco TAC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Enterprise (UCCE) versão v12.5
- Cisco Package Contact Center Enterprise (PCCE) versão v12.5
- Cisco Finesse v12.5
- Cisco Unified Intelligence Center v12.5

Componentes Utilizados

As informações neste documento são baseadas na administração do sistema operacional CVOS - Gerenciamento de certificados.

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

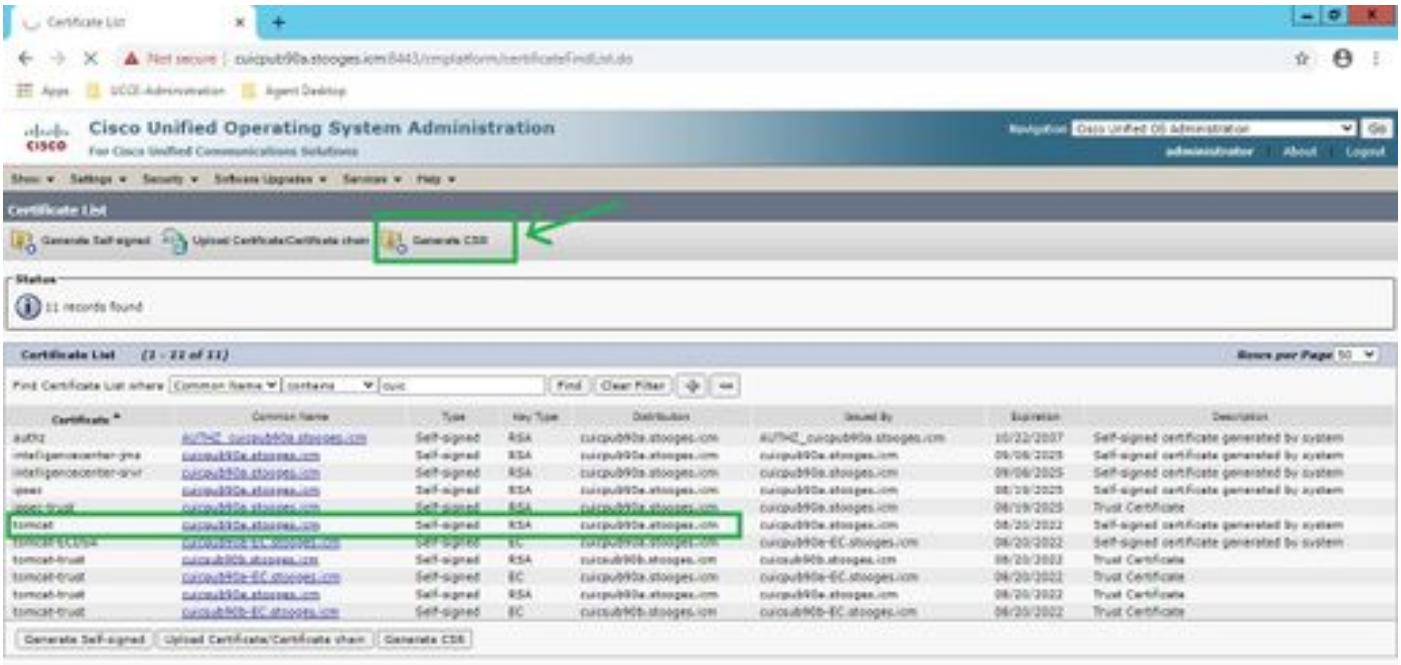
Com certificados SAN de vários servidores, somente um CSR deve ser assinado pela CA para um cluster de nós, em vez do requisito de obter um CSR de cada nó de servidor do cluster e, em seguida, obter um certificado assinado pela CA para cada CSR e gerenciá-los individualmente.

Antes de tentar essa configuração, verifique se esses serviços estão ativos e funcionais:

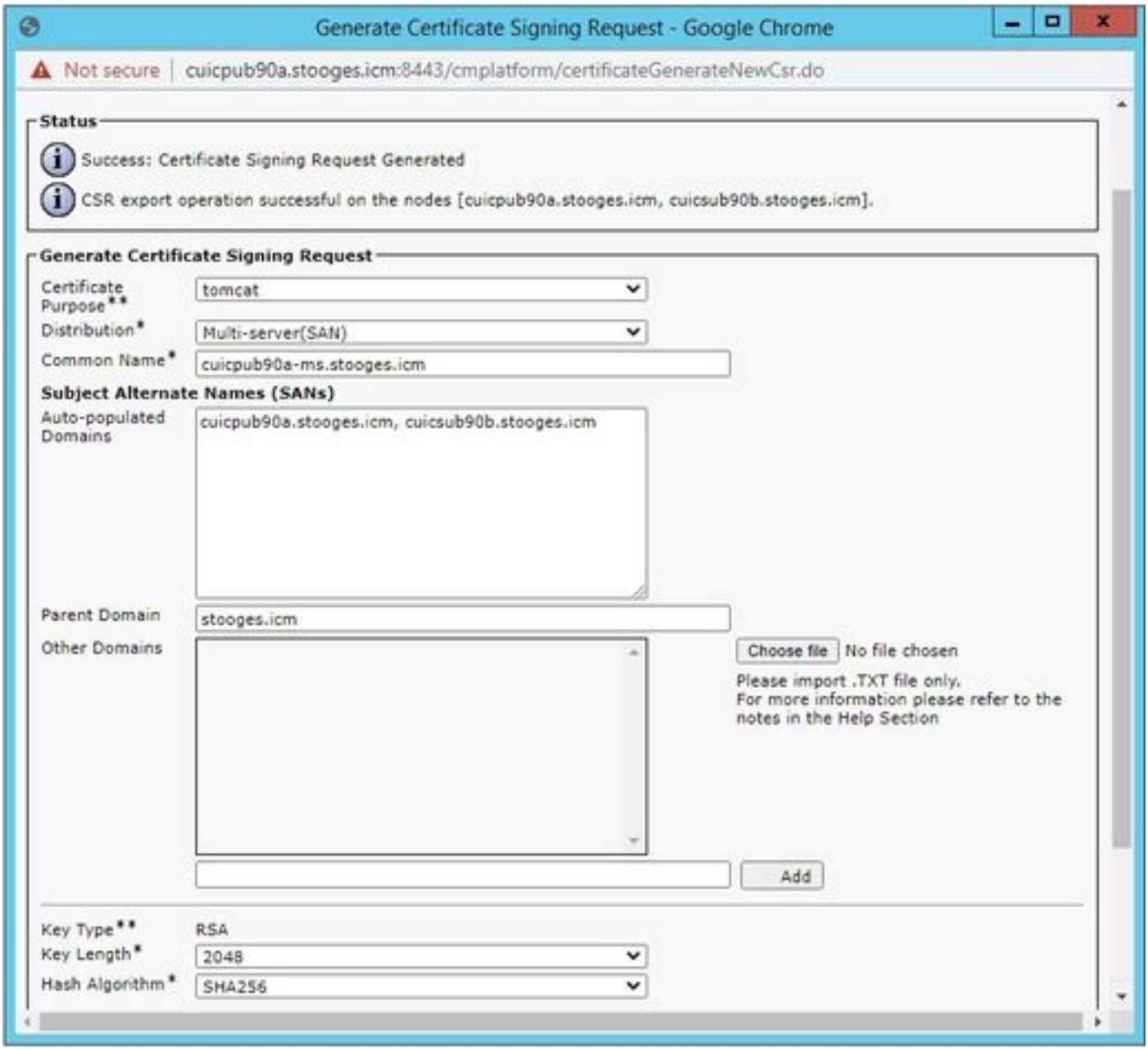
- Serviço Cisco Tomcat
- Notificação de alteração de certificado da Cisco
- Monitor de expiração de certificado da Cisco

Configurar

Etapa1. Efetue login na Administração do Sistema Operacional (OS) e navegue para Segurança > Gerenciamento de Certificado > Gerar CSR como mostrado na imagem.

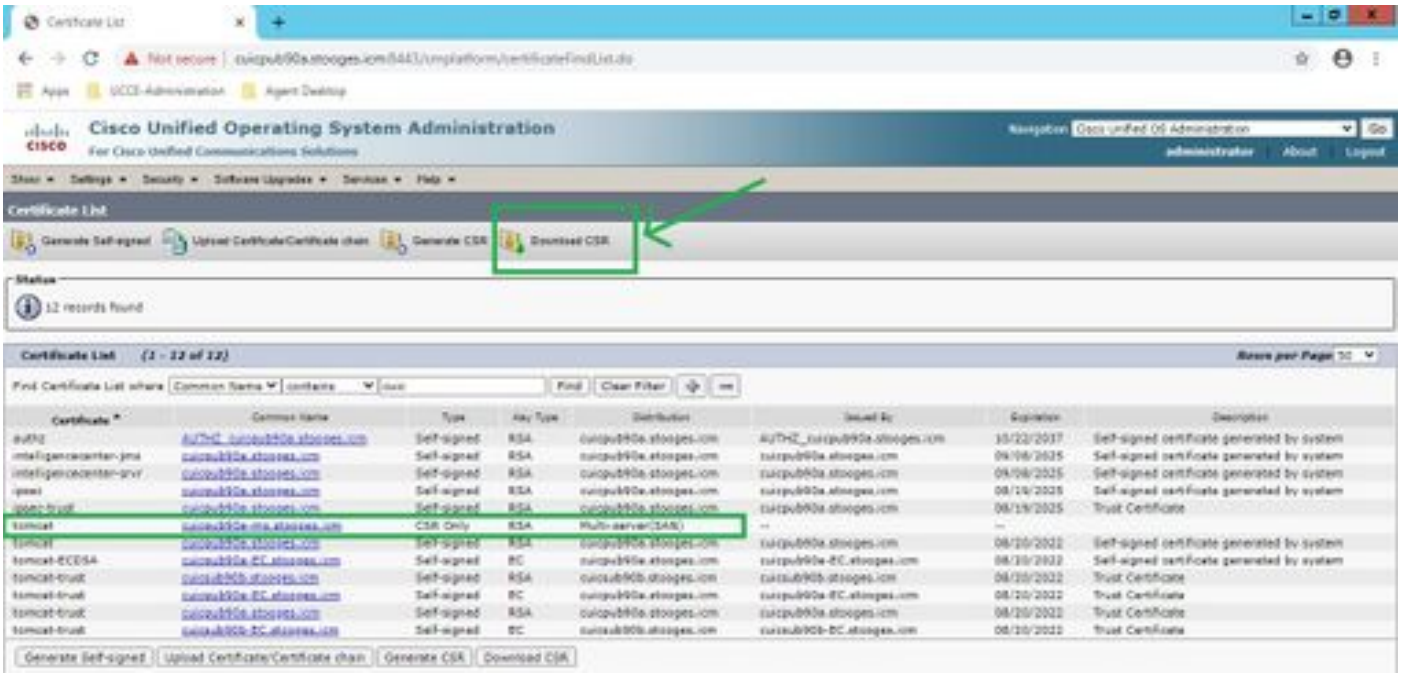


Etapa 2. Selecione Multi-Server SAN em Distribution (Distribuição). Ele preenche automaticamente os domínios SAN e o domínio pai.

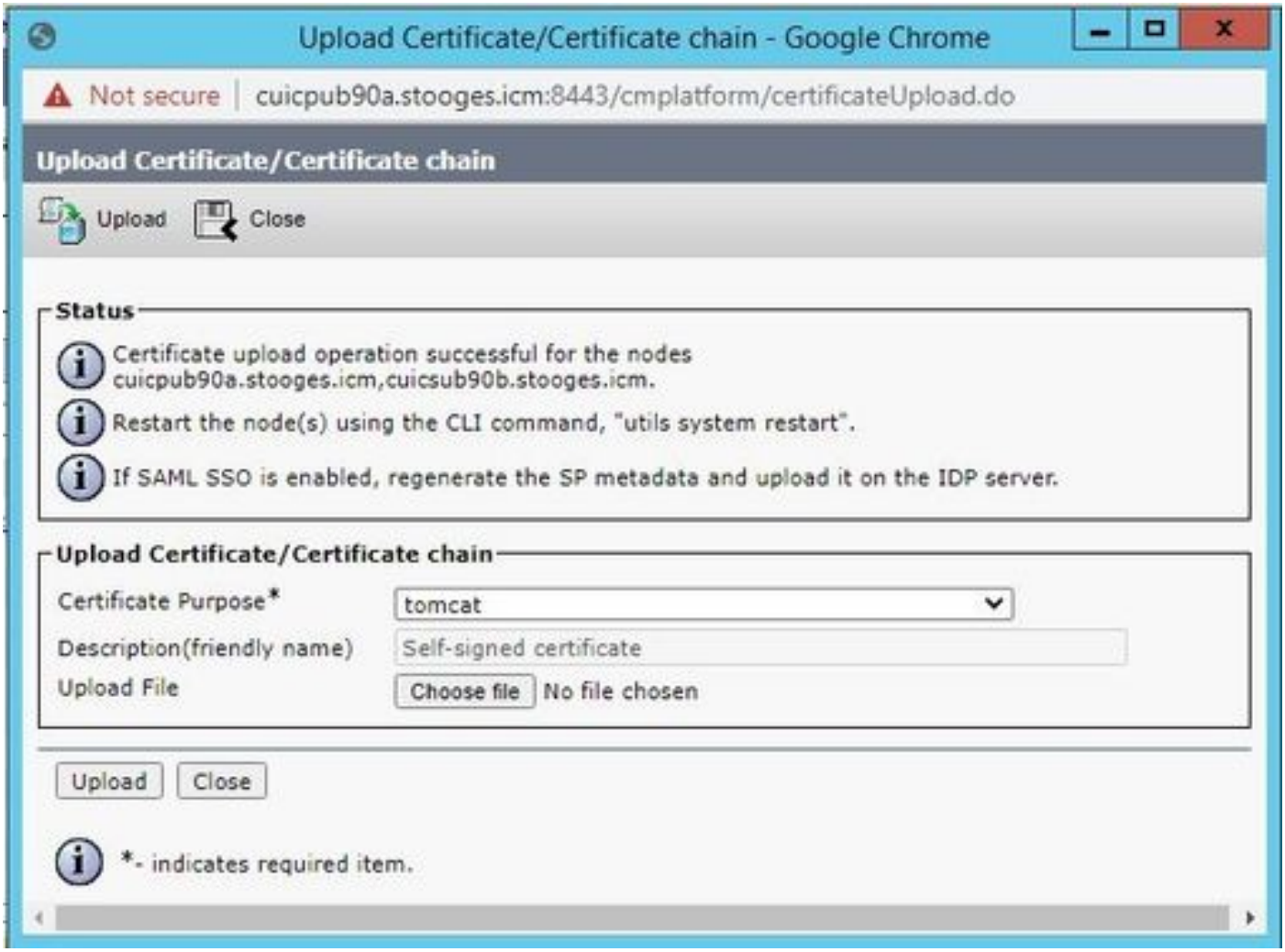


Etapa 3. A geração bem-sucedida de CSR mostra esta mensagem:

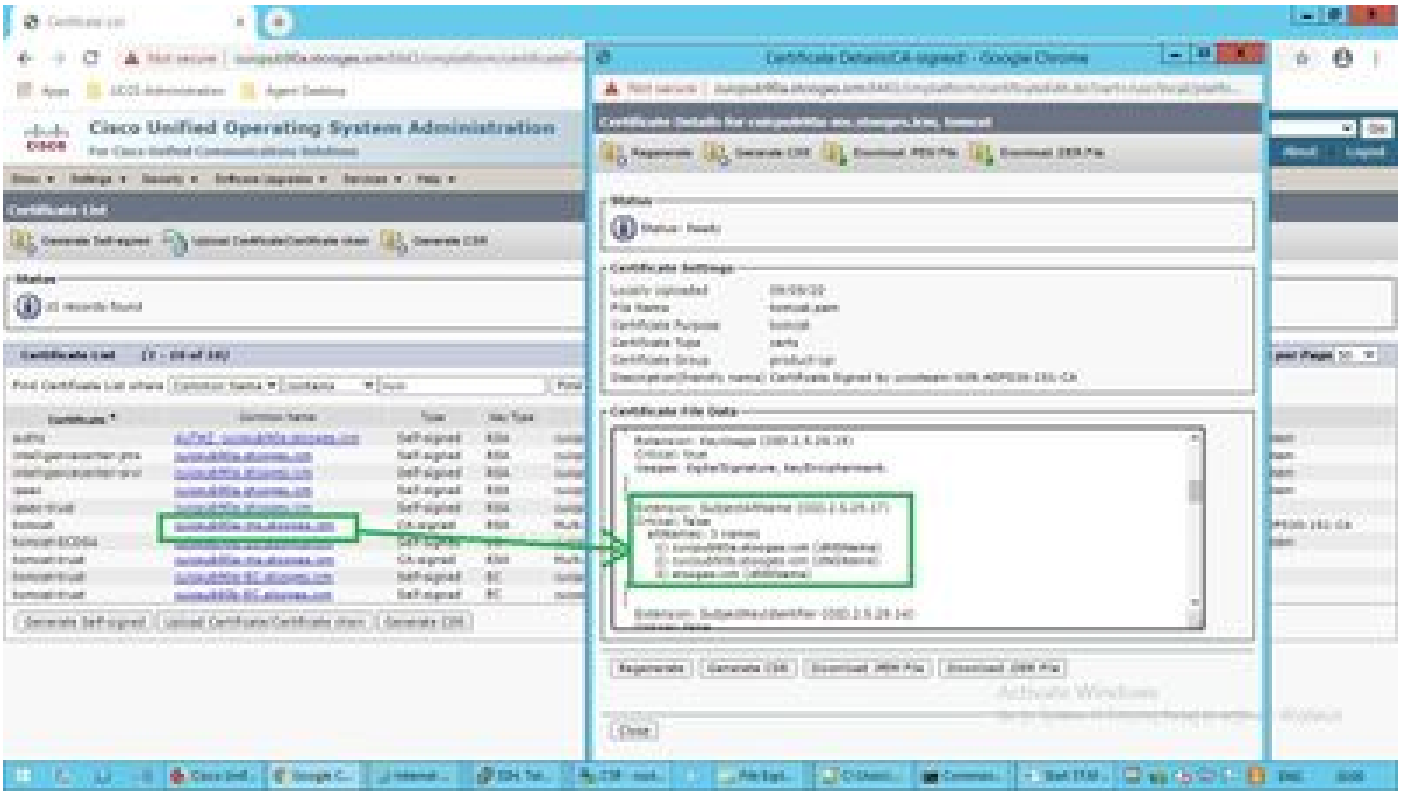
Etapa 4. Após a geração bem-sucedida do CSR, o CSR gerado pode ser visto aqui, que pode ser baixado para ser enviado ao CA para assinatura.



Etapa 5. Carregue o certificado assinado pela CA como tipo tomcat no nó do Publicador do cluster na página de gerenciamento de certificados e siga as instruções exibidas após o carregamento bem-sucedido.



Etapa 6. Após o upload bem-sucedido do arquivo, verifique a lista de certificados que mostra o novo certificado assinado pela CA como tipo multi-SAN.



Clique no novo certificado multi-SAN e verifique se SubjectAltNames mostra o nome do domínio e os FQDNs de todos os nós de cluster.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Faça login na página cmplatform dos nós do assinante e verifique se o mesmo certificado multi-SAN é preenchido com o uso de http://<any-node-fqdn>:8443/cmplatform.

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Colete esses registros de gerenciamento de certificados do acesso à CLI e abra o caso com o Cisco TAC: file get ativelog platform/log/cert*

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.