Guia de gerenciamento certificado da solução UCCX

Índice

Introdução
Pré-requisitos
Requisitos
FQDN, DNS, e domínios
Componentes Utilizados
Informações de Apoio
Configurar
Diagrama da configuração
Certificados assinados
Instale Certificados assinados do aplicativo de Tomcat
Certificados auto-assinados
Integração e configuração de cliente
UCCX-a-MediaSense
MediaSense-à-fineza
UCCX-a-SocialMiner
Certificado de cliente do AppAdmin UCCX
Certificado de cliente da plataforma UCCX
Certificado de cliente do serviço de notificação
Certificado de cliente da fineza
Certificado de cliente de SocialMiner
Certificado de cliente CUIC
Aplicativos de terceiros acessíveis dos scripts
Verificar
Troubleshooting
Problema - Usuário inválido - identificação /Password
Causas
Solução
Problema - O CSR SAN e certificado SAN não combina
Causas
Solução
Problema - REDE:: ERR_CERT_COMMON_NAME_INVALID
Causas
Solução
Mais informações
Defeitos do certificado
Informações Relacionadas

Introdução

Este documento descreve como configurar o Cisco Unified Contact Center Express (UCCX) para o uso do auto-assinado e certificados assinados.

Pré-requisitos

Requisitos

Antes que você continue com as etapas de configuração que estão descritas neste documento, assegure-se de que você tenha o acesso à página de administração do operating system (OS) para estes aplicativos:

- UCCX
- SocialMiner
- MediaSense

Um administrador deve igualmente ter o acesso à loja do certificado no cliente PC do agente e do supervisor.

FQDN, DNS, e domínios

Exige-se que todos os server na configuração UCCX estejam instalados com server e Domain Name do Domain Name System (DNS). Igualmente exige-se que os agentes, os supervisores, e os administradores alcançam os aplicativos da configuração UCCX através do nome de domínio totalmente qualificado (FQDN).

A versão 10.0+ UCCX exige que o Domain Name e os servidores DNS estejam povoados em cima da instalação. Os Certificados que são gerados pelo instalador da versão 10.0+ UCCX contêm o FQDN, como apropriado. Adicionar os servidores DNS e um domínio ao conjunto UCCX antes que você promova à versão 10.0+ UCCX.

Se o domínio muda ou é povoado pela primeira vez, os Certificados devem ser regenerados. Depois que você adiciona o Domain Name à configuração do servidor, regenere todos os Certificados de Tomcat antes que você os instale nos outros pedidos, nos navegadores cliente, ou em cima da geração da solicitação de assinatura de certificado (CSR) para assinar.

Componentes Utilizados

A informação descrita neste documento é baseada nestes componentes de hardware e de software:

- Serviços de Web UCCX
- Serviço de notificação UCCX
- Plataforma Tomcat UCCX
- Fineza Tomcat de Cisco
- Cisco unificou o centro da inteligência (CUIC) Tomcat
- SocialMiner Tomcat
- Serviços de Web de MediaSense

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 a introdução de fineza co-residente e de CUIC, a integração entre UCCX e SocialMiner para o email e o bate-papo, e o uso de MediaSense a fim gravar, compreenda, e instale Certificados através da fineza, a capacidade para pesquisar defeitos edições do certificado é agora criticamente importante.

Este documento descreve o uso do auto-assinado e certificados assinados no ambiente de configuração UCCX que cobre:

- Serviços de notificação UCCX
- Serviços de Web UCCX
- Scripts UCCX
- Fineza co-residente
- CUIC co-residente (dados vivos e relatório histórico)
- MediaSense (gravação e colocação de etiquetas Fineza-baseadas)
- SocialMiner (bate-papo)

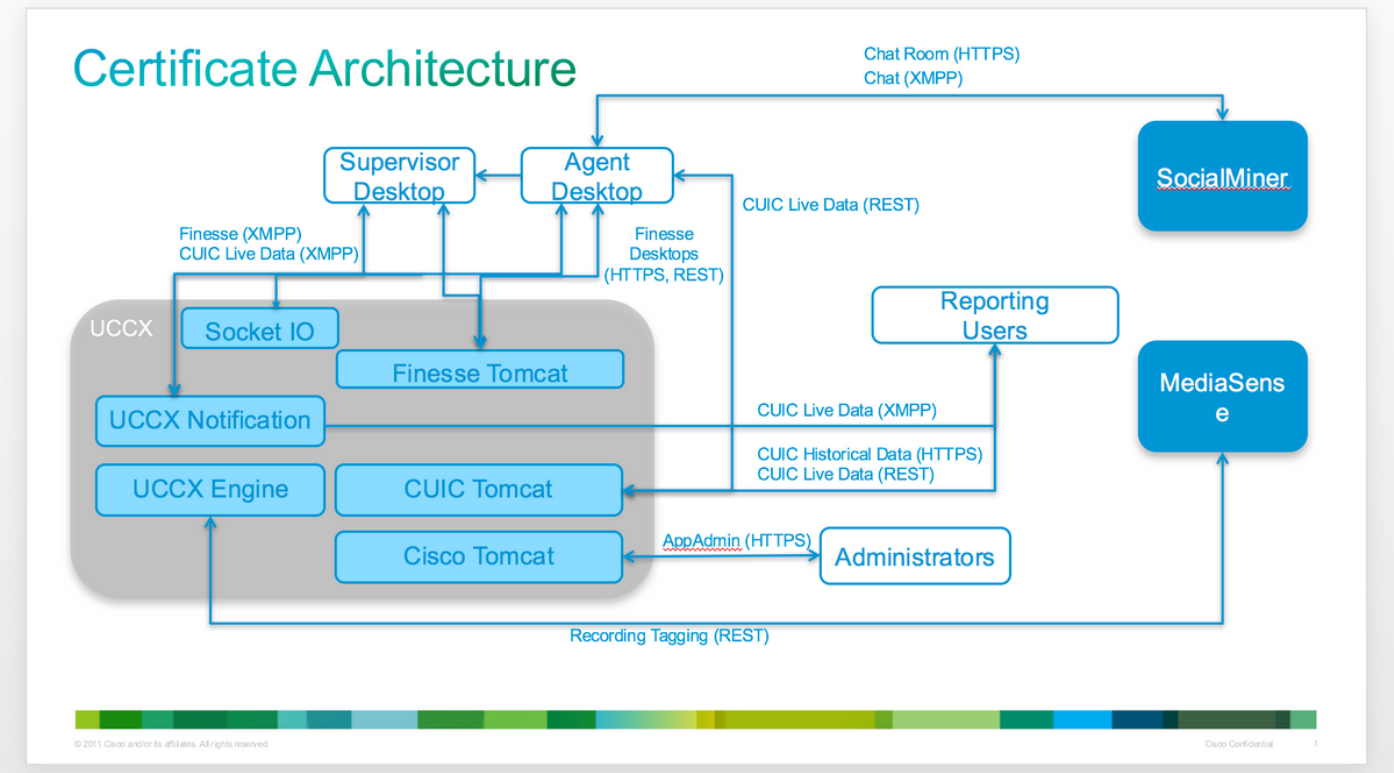
Os Certificados, assinados ou auto-assinados, devem ser instalados em ambos os aplicativos (server) na configuração UCCX, assim como em desktop de cliente do agente e do supervisor.

No sistema operacional das comunicações unificadas (UCOS) 10.5, os Certificados de multi-server foram adicionados de modo que um único CSR pudesse ser gerado para um conjunto em vez de ter que assinar um certificado individual para cada nó no conjunto. Este tipo de certificado é explicitamente unsupported para UCCX, MediaSense, e SocialMiner.

Configurar

Esta seção descreve como configurar o UCCX para o uso do auto-assinado e certificados assinados.

Diagrama da configuração



Certificados assinados

O método recomendada do gerenciamento certificado para a configuração UCCX é leverage certificados assinados. Estes Certificados podem ser assinados por um Certificate Authority (CA) interno ou por CA da terceira conhecido.

Em navegadores principais, tais como Mozilla Firefox e internet explorer, os certificados de raiz para CA da terceira conhecidos são instalados à revelia. Os Certificados para os aplicativos da configuração UCCX que são assinados por estes CA são confiados à revelia, como suas extremidades do certificate chain em um certificado de raiz que seja instalado já no navegador.

O certificado de raiz de CA interno pôde igualmente ser instalado no navegador cliente com uma política do grupo ou a outra configuração atual.

Você pode escolher se ter os Certificados do aplicativo da configuração UCCX assinados por CA da terceira conhecido ou por CA interno baseado na Disponibilidade e na instalação provisória do certificado de raiz para os CA no navegador cliente.

Instale Certificados assinados do aplicativo de Tomcat

Termine estas etapas para cada nó da publisher e subscriber UCCX, do SocialMiner, e dos aplicativos da administração da publisher e subscriber de MediaSense:

1. Navegue à **página de administração do OS** e escolha o **> gerenciamento de certificado da Segurança**.
2. O clique **gerencie o CSR**.
3. Da lista de drop-down da **lista do certificado**, escolha **TomCat** como o nome do certificado e o clique **gerencie o CSR**.
4. Navegue ao **> gerenciamento de certificado da Segurança** e escolha a **transferência CSR**.
5. Da janela pop-up, escolha **TomCat da** lista de drop-down e clique a **transferência CSR**.

Envie o CSR novo a CA da terceira ou assine-o com CA interno, como descrito anteriormente. Este processo deve produzir estes certificados assinados:

- Certificado de raiz para CA
- Certificado do aplicativo do editor UCCX
- Certificado do aplicativo do subscritor UCCX
- Certificado do aplicativo de SocialMiner
- Certificado do aplicativo do editor de MediaSense
- Certificado do aplicativo do subscritor de MediaSense

Nota: Saa do campo da **distribuição no** CSR como o FQDN do server. Não o mude ao "Multi-server (SAN)" porque os Certificados de multi-server não são apoiados com UCCX, MediaSense, ou SocialMiner.

Termine estas etapas em cada server de aplicativo a fim transferir arquivos pela rede o certificado de raiz e o certificado do aplicativo aos Nós:

Nota: Se você transfere arquivos pela rede os Certificados da raiz e do intermediário em um editor (UCCX ou MediaSense), deve automaticamente ser replicated ao subscritor. Não há nenhuma necessidade de transferir arquivos pela rede os Certificados da raiz ou do intermediário nos outro, server do NON-editor na configuração se todos os Certificados do aplicativo são assinados através do mesmo certificate chain.

1. Navegue à **página de administração do OS** e escolha o **> gerenciamento de certificado da Segurança**.
2. Clique o **certificado da transferência de arquivo pela rede**.
3. Transfira arquivos pela rede o certificado de raiz e escolha a Tomcat-**confiança** como o tipo do certificado.
4. Clique o **arquivo da transferência de arquivo pela rede**.
5. Clique o **certificado da transferência de arquivo pela rede**.
6. Transfira arquivos pela rede o certificado do aplicativo e escolha **TomCat** como o tipo do certificado.
7. Clique o **arquivo da transferência de arquivo pela rede**. Nota: Se CA subordinado assina o certificado, transfira arquivos pela rede o certificado de raiz de CA subordinado como o certificado da Tomcat-*confiança* em vez do certificado de raiz. Se um certificado intermediário é emitido, transfira arquivos pela rede este certificado à loja da Tomcat-*confiança* além do que o certificado do aplicativo.
8. Uma vez que completo, reinicie estes aplicativos: Publisher e subscriber de Cisco MediaSenseCisco SocialMinerPublisher e subscriber de Cisco UCCX

Nota: Quando você usa UCCX, MediaSense, e SocialMiner 11.5 e mais atrasado, há um certificado novo chamado Tomcat-ECDSA. Quando você transfere arquivos pela rede um certificado assinado de Tomcat-ECDSA ao server, transfira arquivos pela rede o certificado do aplicativo como um certificado de Tomcat-ECDSA--não um certificado de TomCat. Para mais informações sobre de ECDSA, refira a seção Informação Relacionada para o link para compreender e configurar Certificados ECDSA.

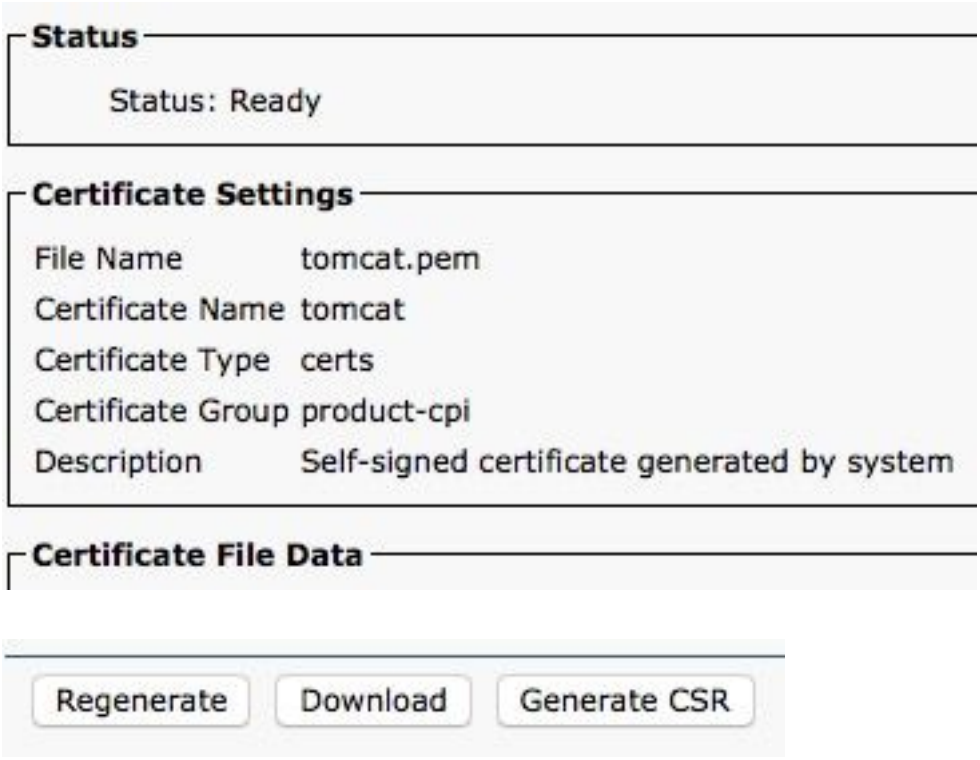
Certificados auto-assinados

Todos os Certificados que são usados na configuração UCCX vêm instalado nos aplicativos da configuração e auto-são assinados. Estes certificados auto-assinados não são confiados implicitamente quando apresentados a um navegador cliente ou a um outro aplicativo da configuração. Embora se recomende assinar todos os Certificados na configuração UCCX, você pode usar os certificados auto-assinados instalados.

Para cada relacionamento do aplicativo, você deve transferir o certificado apropriado e transferi-lo arquivos pela rede ao aplicativo. Termine estas etapas a fim obter e transferir arquivos pela rede os Certificados:

1. Alcance a **página de administração do OS do** aplicativo e escolha o **> gerenciamento de certificado da Segurança**.

2. Clique o arquivo apropriado do **.pem do** certificado e escolha a **transferência**:



3. A fim transferir arquivos pela rede um certificado no aplicativo apropriado, navegue à **página de administração do OS** e escolha o **> gerenciamento de certificado da Segurança**.
4. Clique o **certificado/certificate chain da transferência de arquivo pela rede:**

5. Uma vez que completo, reinicie estes server:

   Publisher e subscriber de Cisco MediaSenseCisco SocialMinerPublisher e subscriber de Cisco UCCX

A fim instalar certificados auto-assinados na máquina cliente, use um gerente da política ou do pacote do grupo, ou instale-os individualmente no navegador de cada agente PC.

Para o internet explorer, instale os certificados auto-assinados do lado do cliente na loja das **Autoridades de certificação de raiz confiável**.

Para Mozilla Firefox, termine estas etapas:

1. Navegue às **ferramentas > às opções**.
2. Clique na guia Advanced.
3. Clique **Certificados da vista**.
4. Navegue à aba dos **server**.
5. O clique **adiciona a exceção**.

Integração e configuração de cliente

UCCX-a-MediaSense

O UCCX consome a interface de programação de aplicativo do RESTO dos serviços de Web de MediaSense (API) para duas finalidades:

- A fim subscrever às notificações das gravações novas que são invocadas no gerente das comunicações unificadas de Cisco (CUCM).
- A fim etiquetar gravações de agentes UCCX com o agente e contactar a informação da fila de serviços (CSQ).

O UCCX consome o RESTO API nos Nós da administração de MediaSense. Há um máximo de dois em todo o conjunto de MediaSense. O UCCX não conecta através do RESTO API aos Nós da expansão de MediaSense. Ambos os Nós UCCX devem consumir o RESTO API de MediaSense, assim que instale os dois Certificados de MediaSense Tomcat em ambos os Nós UCCX.

Transfira arquivos pela rede a corrente assinada ou de certificado auto-assinado dos server de MediaSense ao keystore da Tomcat-*confiança* UCCX.

MediaSense-à-fineza

MediaSense consome o RESTO API dos serviços de Web da fineza a fim autenticar agentes para o dispositivo da busca e do jogo de MediaSense na fineza.

O server de MediaSense configurado na disposição da fineza XML para o dispositivo da busca e do jogo deve consumir o RESTO API da fineza, assim que instale os dois Certificados UCCX Tomcat nesse nó de MediaSense.

Transfira arquivos pela rede a corrente assinada ou de certificado auto-assinado dos server UCCX ao keystore da Tomcat-*confiança de* MediaSense.

UCCX-a-SocialMiner

O UCCX consome o RESTO de SocialMiner e a notificação API a fim controlar contatos e configuração do email. Ambos os Nós UCCX devem consumir o RESTO API de SocialMiner e ser notificados pelo serviço de notificação de SocialMiner, assim que instale o certificado de SocialMiner Tomcat em ambos os Nós UCCX.

Transfira arquivos pela rede a corrente assinada ou de certificado auto-assinado do server de SocialMiner ao keystore da Tomcat-*confiança* UCCX.

Certificado de cliente do AppAdmin UCCX

O certificado de cliente do AppAdmin UCCX é usado para a administração do sistema UCCX. A fim instalar o certificado do AppAdmin UCCX para administradores UCCX, no PC cliente, navegue a **https:// <UCCX FQDN>/appadmin/main** para cada um dos Nós UCCX e instale o certificado através do navegador.

Certificado de cliente da plataforma UCCX

Os serviços de Web UCCX são usados para a entrega de contatos do bate-papo aos navegadores cliente. A fim instalar o certificado da plataforma UCCX para agentes e supervisores UCCX, no PC cliente, navegue a **https:// <UCCX FQDN>/appadmin/main** para cada um dos Nós UCCX e instale o certificado através do navegador.

Certificado de cliente do serviço de notificação

O serviço de notificação CCX é usado pela fineza, pelo UCCX, e pelo CUIC a fim enviar a informação em tempo real ao desktop de cliente através do protocolo elástico da Mensagem e da presença (XMPP). Isto é usado para uma comunicação da fineza do tempo real assim como CUIC vivem dados.

A fim instalar o certificado de cliente do serviço de notificação no PC dos agentes e dos supervisores ou dos usuários do relatório que usam dados vivos, navegam a **https:// <UCCX FQDN>:7443/** para cada um dos Nós UCCX e instalam o certificado através do navegador.

Certificado de cliente da fineza

O certificado de cliente da fineza é usado pelos desktops da fineza a fim conectar a Tomcat da fineza o exemplo para fins de uma comunicação do RESTO API entre o desktop e o server co-residente da fineza.

A fim instalar o certificado da fineza para agentes e supervisores, no PC cliente, navegue a **https:// <UCCX FQDN>:8445/** para cada um dos Nós UCCX e instale o certificado com as alertas do navegador.

A fim instalar o certificado da fineza para administradores da fineza, no PC cliente, navegue a **https:// <UCCX FQDN>:8445/cfadmin** para cada um dos Nós UCCX e instale o certificado com as alertas do navegador.

Certificado de cliente de SocialMiner

O certificado de SocialMiner Tomcat deve ser instalado na máquina cliente. Uma vez que um agente aceita um pedido do bate-papo, o dispositivo do bate-papo está reorientado a uma URL que represente o chat room. Este chat room é hospedado pelo server de SocialMiner e contém o contato do cliente ou do bate-papo.

A fim instalar o certificado de SocialMiner no navegador, no PC cliente, navegue ao **<SocialMiner FQDN>/de https://** e instale o certificado com as alertas do navegador.

Certificado de cliente CUIC

O certificado CUIC Tomcat deve ser instalado na máquina cliente para agentes, supervisores, e os usuários do relatório que usam a interface da WEB CUIC para relatórios de histórico ou vivem dados relatam dentro do página da web CUIC ou dentro dos dispositivos no desktop.

A fim instalar o certificado CUIC Tomcat no navegador, no PC cliente, navegue a **https:// <UCCX FQDN>:8444/** e instale o certificado com as alertas do navegador.

CUIC vivem o certificado dos dados (desde 11.x)

O CUIC usa o serviço do soquete IO para os dados vivos backend. Este certificado deve ser instalado na máquina cliente para agentes, supervisores e usuários do relatório que usam a interface da WEB CUIC para dados Live ou que usam os dispositivos vivos dos dados dentro da fineza.

A fim instalar o certificado do soquete IO no navegador, no PC cliente, navegue a **https:// <UCCX FQDN>:12015/** e instale o certificado com as alertas do navegador.

Aplicativos de terceiros acessíveis dos scripts

Se um script UCCX é projetado a fim alcançar um lugar seguro em um server da terceira (por exemplo, *obtenha a* etapa do *documento URL a um* HTTPS URL ou *faça o atendimento do resto a um* RESTO URL HTTPS), transfira arquivos pela rede a corrente assinada ou de certificado auto-assinado do serviço de terceira parte ao keystore da Tomcat-*confiança* UCCX. A fim obter este certificado, alcance a **página de administração do OS** UCCX e escolha o **certificado da transferência de arquivo pela rede**.

O motor UCCX está configurado a fim procurar o keystore de Tomcat da plataforma por certificates chain da terceira quando apresentado com estes Certificados por aplicativos de terceiros quando alcançam lugar seguros através das etapas do script.

O certificate chain inteiro deve ser transferido arquivos pela rede ao keystore de Tomcat da plataforma, acessível através da **página de administração do OS**, porque o keystore de Tomcat não contém nenhum certificado de raiz à revelia.

Depois que você termina estas ações, reinicie o motor de Cisco UCCX.

Verificar

A fim verificar que todos os Certificados estão instalados corretamente, você pode testar as características que são descritas nesta seção. Se nenhum erro do certificado aparece e todas as características funcionam corretamente, os Certificados estão instalados corretamente.

- Configurar a fineza de modo que grave automaticamente um agente através dos trabalhos. Depois que um atendimento é segurado pelo agente, use o aplicativo da busca e do jogo de MediaSense a fim encontrar o atendimento. Verifique que o atendimento tem o agente, um CSQ, e as etiquetas da equipe anexadas aos metadata da gravação em MediaSense.
- Configurar o bate-papo da Web do agente com SocialMiner. Injete um contato do bate-papo através do formulário da Web. Verifique que o agente recebe a bandeira para aceitar o contato do bate-papo e para verificar igualmente que o contato do bate-papo está aceitado uma vez, as cargas do formulário do bate-papo corretamente e o agente pode receber e

enviar mensagens do bate-papo.
- Tentativa de entrar um agente através da fineza. Verifique que nenhum aviso do certificado aparece e que o página da web não alerta para a instalação dos Certificados no navegador. Verifique que o agente pode mudar estados corretamente e um atendimento novo em UCCX é apresentado corretamente ao agente.
- Depois que você configura os dispositivos vivos dos dados na disposição do desktop da fineza do agente e do supervisor, entre um agente, um supervisor, e um usuário do relatório. Verifique que os dispositivos vivos dos dados carregam corretamente, que os dados iniciais estão povoados no dispositivo, e que os dados refrescam quando os dados subjacentes mudarem.
- Tente conectar de um navegador ao AppAdmin URL em ambos os Nós UCCX. Verifique que nenhum aviso do certificado aparece quando alertado com a página de login.

Troubleshooting

Problema - Usuário inválido - identificação /Password

Os agentes da fineza UCCX são incapazes de entrar com erro “**usuário inválido - a identificação /Password**”.

Causas

O CCX unificado joga uma exceção “SSLHandshakeException “e não estabelece uma conexão com o CM unificado.

Solução

- Verifique que o certificado unificado CM Tomcat não está expirado.
- Assegure-se de que todo o certificado que você transfira arquivos pela rede no CM unificado tenha qualquer destes Ramais marcados como crítico:
  Uso da chave X509v3 (OID - 2.5.29.15)
  Limitações X509v3 básicas (OID - 2.5.29.19)
  Se você marca quaisquer outros Ramais como críticos, a comunicação falha entre o CCX unificado e o CM unificado devido à falha da verificação de certificado unificada CM.

Problema - O CSR SAN e certificado SAN não combina

A transferência de arquivo pela rede de um certificado assinado de CA indica o erro “CSR SAN e o certificado SAN não combina”.

Causas

CA pôde ter adicionado um outro domínio do pai no campo alternativo dos nomes do assunto do certificado (SAN). À revelia, o CSR terá estes sem:

SubjectAltName [
  example.com (dNSName)

hostname.example.com (dNSName)
]

Os CA puderam retornar um certificado com um outro SAN adicionado ao certificado: www.hostname.example.com. O certificado terá um SAN extra neste caso:

SubjectAltName [
example.com (dNSName)
hostname.example.com (dNSName)

www.hostname.example.com (dNSName)
]

Isto causa o erro da má combinação SAN.

Solução

"Na seção do nome alternativo sujeito (sem)" da página da solicitação de assinatura de certificado UCCX "gerencia", gerenciem o CSR com um campo vazio do domínio do pai. Esta maneira o CSR não é gerada com um atributo SAN, CA pode formatar sem, e não haverá uma má combinação do atributo SAN quando você transfere arquivos pela rede o certificado a UCCX. Note que o campo do domínio do pai opta o domínio do server UCCX, assim que o valor deve explicitamente ser removido quando os ajustes para o CSR forem configurados.

Problema - REDE:: ERR_CERT_COMMON_NAME_INVALID

Quando você alcança todo o página da web UCCX, de MediaSense, ou de SocialMiner, você recebe um Mensagem de Erro.

"Sua conexão não é privada.

Os atacantes puderam tentar roubar sua informação do <Server_FQDN> (por exemplo, senhas, mensagens, ou cartões de crédito). REDE:: ERR_CERT_COMMON_NAME_INVALID

Este server não poderia mostrar que é <Server_FQDN>; seu Security Certificate é do [missing_subjectAltName]. Isto pode ser causado por um misconfiguration ou por um atacante que interceptam sua conexão."

Causas

A versão 58 de Chrome introduziu uns recursos de segurança novos onde relatasse que o certificado de um Web site não é seguro se seu Common Name (CN) não é incluído igualmente como um SAN.

Solução

- Você pode navegar a **avançado > continua ao <Server_FQDN> (inseguro)** a fim continuar ao local e aceitar o erro do certificado.
- Você pode evitar o erro completamente com certificados assinados de CA. Quando você

gerencie um CSR, o FQDN do server está incluído como um SAN. CA pode assinar o CSR, e depois que você transfere arquivos pela rede o certificado assinado de volta ao server, o certificado de server terá o FQDN no campo SAN de modo que o erro não seja apresentado.

Mais informações

Veja a seção “remover o apoio para o commonName que combina nos Certificados” nos Deprecations e nas remoções em Chrome 58.

Certificate defeitos

- Identificação de bug Cisco CSCvb46250 - UCCX: Impacto do certificado de Tomcat ECDSA em dados vivos da fineza
- Identificação de bug Cisco CSCvb58580 - Incapaz de entrar a SocialMiner com ambo o TomCat e a Tomcat-ECDSA assinou por RSA CA
- Identificação de bug Cisco CSCvd56174 - UCCX: Falha de login do agente da fineza devido a SSLHandshakeException
- Identificação de bug Cisco CSCuv89545 - Vulnerabilidade do atasco da fineza

Informações Relacionadas

- Compreenda Certificados ECDSA em uma solução UCCX
- UCCX assinado e exemplo de configuração dos certificados auto-assinados
- Suporte Técnico e Documentação - Cisco Systems