Guía de administración de certificados de la solución UCCX

Contenido

Introducción

Este documento describe cómo configurar el Cisco Unified Contact Center Express (UCCX) para el uso de uno mismo-firmado y los certificados firmados.

Prerrequisitos

Requisitos

Antes de que usted proceda con los pasos para la configuración que se describen en este documento, asegúrese de que usted tenga acceso a la página de administración del operating system (OS) para estas aplicaciones:

- UCCX
- SocialMiner
- MediaSense

Un administrador debe también tener acceso al almacén de certificados en el cliente PC del agente y del supervisor.

FQDN, DNS, y dominios

Se requiere que todos los servidores en la configuración UCCX estén instalados con los servidores y los Domain Name del Domain Name System (DNS). También se requiere que los agentes, los supervisores, y los administradores acceden las aplicaciones de la configuración UCCX vía el nombre de dominio completo (FQDN).

La versión 10.0+ UCCX requiere que pueblen el Domain Name y a los servidores DNS tras la instalación. Los Certificados que son generados por el instalador de la versión 10.0+ UCCX contienen el FQDN, como apropiado. Agregue los servidores DNS y un dominio al cluster UCCX antes de que usted actualice a la versión 10.0+ UCCX.

Si el dominio cambia o se puebla por primera vez, los Certificados deben ser regenerados. Después de que usted agregue el Domain Name a la Configuración del servidor, regenere todos los Certificados de Tomcat antes de que usted los instale en las otras aplicaciones, en los buscadores del cliente, o sobre la generación del pedido de firma de certificado (CSR) para firmar.

Componentes Utilizados

La información descrita en este documento se basa en estos componentes de hardware y de software:

- Servicios web UCCX
- Servicio de notificación UCCX
- Plataforma Tomcat UCCX
- Delicadeza Tomcat de Cisco
- Cisco unificó el centro de la inteligencia (CUIC) Tomcat
- SocialMiner Tomcat
- Servicios web de MediaSense

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando,

asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Con la introducción de delicadeza del coresidente y de CUIC, la integración entre UCCX y SocialMiner para el correo electrónico y la charla, y el uso de MediaSense para registrar, entienda, y instale los Certificados vía la delicadeza, la capacidad de resolver problemas los problemas del certificado es críticamente importante ahora.

Este documento describe el uso de uno mismo-firmado y los certificados firmados en el entorno de configuración UCCX que cubre:

- Servicios de notificación UCCX
- Servicios web UCCX
- Scripts UCCX
- Delicadeza del coresidente
- Coresidente CUIC (datos vivos e información histórica)
- MediaSense (grabación y el marcar con etiqueta Delicadeza-basados)
- SocialMiner (charla)

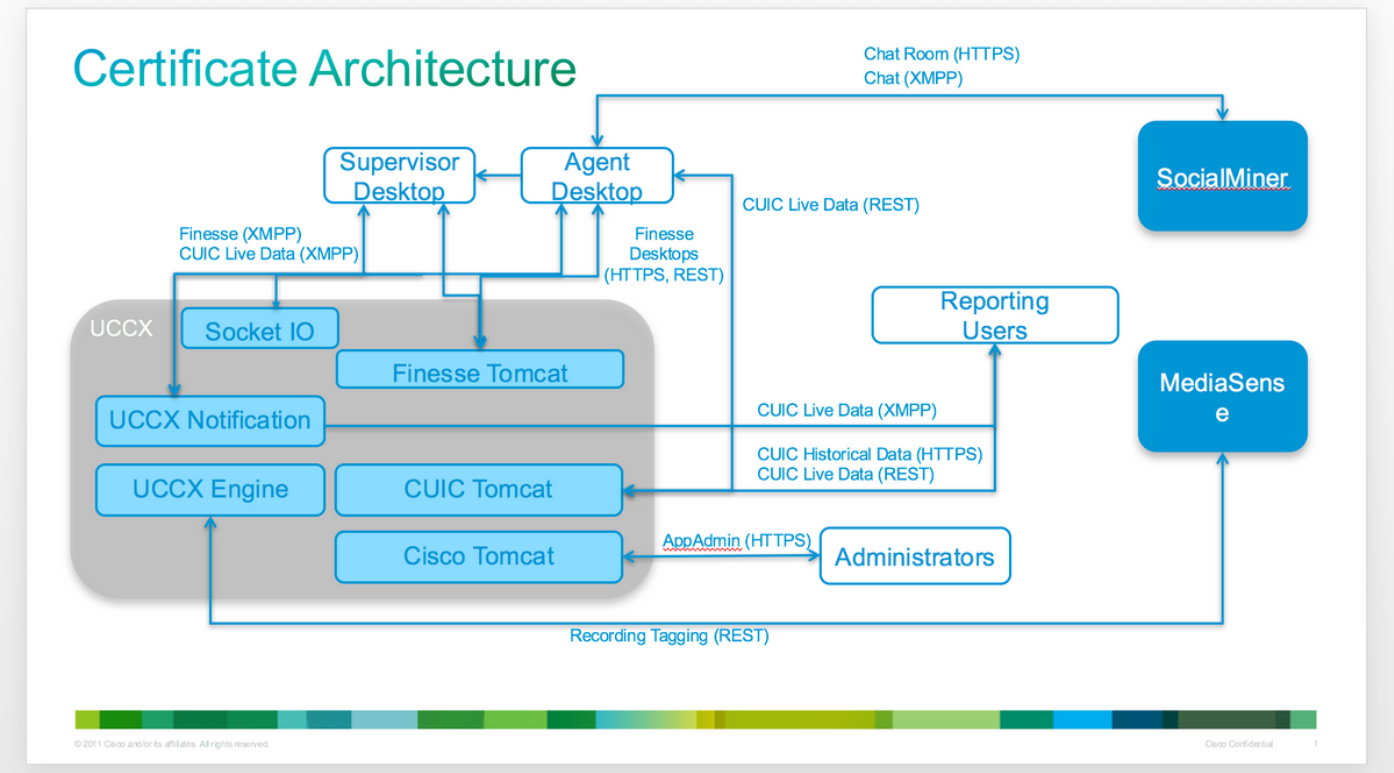
Los Certificados, firmados o uno mismo-firmados, se deben instalar en ambas las aplicaciones (servidores) en la configuración UCCX, así como los escritorios del cliente del agente y del supervisor.

En el sistema operativo de las Comunicaciones unificadas (UCOS) 10.5, los Certificados multiservidores fueron agregados de modo que un solo CSR se pudiera generar para un cluster en vez de tener que firmar un certificado individual para cada nodo en el cluster. Este tipo de certificado está explícitamente sin apoyo para UCCX, MediaSense, y SocialMiner.

Configurar

Esta sección describe cómo configurar el UCCX para el uso de uno mismo-firmado y los certificados firmados.

Diagrama de la configuración



Certificados firmados

El método recomendado de administración de certificados para la configuración UCCX es leverage los certificados firmados. Estos Certificados se pueden firmar por un Certificate Authority (CA) interno o CA de tercera persona bien conocido.

En los navegadores importantes, tales como Mozilla Firefox y Internet Explorer, los certificados raíz para los CA de tercera persona bien conocidos están instalados por abandono. Los Certificados para las aplicaciones de la configuración UCCX que son firmadas por estos CA se confían en por abandono, como sus extremos de la Cadena de certificados en un certificado raíz que esté instalado ya en el navegador.

El certificado raíz de CA interno se pudo también instalar previamente en el buscador del cliente con la directiva del grupo o la otra configuración actual.

Usted puede elegir si hacer los Certificados de la aplicación de la configuración UCCX firmar por CA de tercera persona bien conocido o por CA interno basado en la Disponibilidad y la preinstalación del certificado raíz para los CA en el buscador del cliente.

Instale los Certificados firmados de la aplicación de Tomcat

Complete estos pasos para cada nodo del editor y suscriptor UCCX, del SocialMiner, y de las aplicaciones de la administración del editor y suscriptor de MediaSense:

1. Navegue a la **página de administración OS** y elija el **Certificate Management (Administración de certificados) de la Seguridad**.
2. El tecleo **genera el CSR**.
3. De la lista desplegable de la **lista del certificado**, elija el **tomcat** como el nombre del certificado y el tecleo **genera el CSR**.
4. Navegue al **Certificate Management (Administración de certificados) de la Seguridad** y elija

la **descarga CSR**.

5. De la ventana emergente, elija el **tomcat de la** lista desplegable y haga clic la **descarga CSR**.

Envíe el nuevo CSR a CA de tercera persona o fírmelo con CA interno, según lo descrito previamente. Este proceso debe presentar estos certificados firmados:

- Certificado raíz para CA
- Certificado de la aplicación UCCX Publisher
- Certificado de la aplicación del suscriptor UCCX
- Certificado de la aplicación de SocialMiner
- Certificado de la aplicación de MediaSense Publisher
- Certificado de la aplicación del suscriptor de MediaSense

Nota: Deje el campo de la **distribución** en el CSR como el FQDN del servidor. No lo cambie a “multiservidor (SAN)” pues los Certificados multiservidores no se soportan con UCCX, MediaSense, o SocialMiner.

Complete estos pasos en cada servidor de aplicaciones para cargar el certificado raíz y el certificado de la aplicación a los Nodos:

Nota: Si usted carga los Certificados de la raíz y del intermedio en un editor (UCCX o MediaSense), debe ser replicado automáticamente al suscriptor. No hay necesidad de cargar los Certificados de la raíz o del intermedio sobre el otro, los servidores de NON-Publisher en la configuración si todos los Certificados de la aplicación se firman vía la misma Cadena de certificados.

1. Navegue a la **página de administración OS** y elija el **Certificate Management (Administración de certificados) de la Seguridad**.
2. Haga clic el **certificado de la carga**.
3. Cargue el certificado raíz y elija la Tomcat-**confianza** como el tipo de certificado.
4. Haga clic el **archivo de la carga**.
5. Haga clic el **certificado de la carga**.
6. Cargue el certificado de la aplicación y elija el **tomcat** como el tipo de certificado.
7. Haga clic el **archivo de la carga**. Nota: Si CA subordinado firma el certificado, cargue el certificado raíz de CA subordinado como el certificado de la Tomcat-*confianza* en vez del certificado raíz. Si se publica un certificado intermedio, cargue este certificado al almacén de la Tomcat-*confianza* además del certificado de la aplicación.
8. Complete, recomience una vez estas aplicaciones: Editor y suscriptor de Cisco MediaSenseCisco SocialMinerEditor y suscriptor de Cisco UCCX

Nota: Cuando usted utiliza UCCX, MediaSense, y SocialMiner 11.5 y posterior, hay un nuevo certificado llamado Tomcat-ECDSA. Cuando usted carga un certificado firmado de Tomcat-ECDSA al servidor, cargue el certificado de la aplicación como certificado de Tomcat-ECDSA--no un certificado del tomcat. Para más información sobre ECDSA, refiera a la sección de información relacionada para el link para entender y para configurar los Certificados ECDSA.

Certificados autofirmados

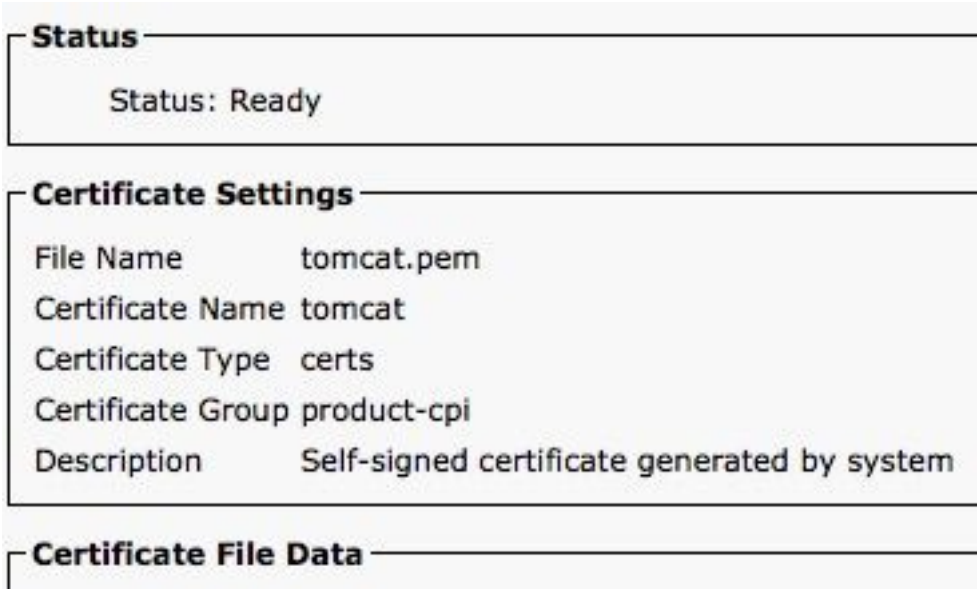
Todos los Certificados que se utilizan en la configuración UCCX vienen instalado previamente en

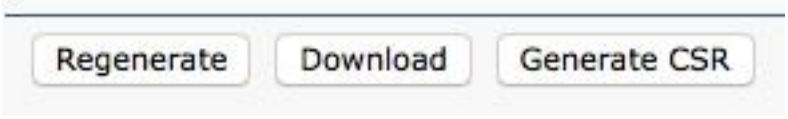
las aplicaciones de la configuración y uno mismo-se firman. Estos certificados autofirmados no se confían en implícito cuando están presentados a un buscador del cliente o a otra aplicación de la configuración. Aunque se recomiende para firmar todos los Certificados en la configuración UCCX, usted puede utilizar los certificados autofirmados instalados previamente.

Para cada relación de la aplicación, usted debe descargar el certificado apropiado y cargarlo a la aplicación. Complete estos pasos para obtener y cargar los Certificados:

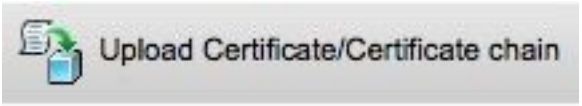
1. Acceda la **página de administración de la** aplicación **OS** y elija el **Certificate Management (Administración de certificados) de la Seguridad**.

2. Haga clic el archivo apropiado del **.pem del** certificado y elija la **descarga**:





3. Para cargar un certificado en la aplicación apropiada, navegue a la **página de administración OS** y elija el **Certificate Management (Administración de certificados) de la Seguridad**.
4. Haga clic el **certificado/la Cadena de certificados de la carga:**



5. Complete, recomience una vez estos servidores:

   Editor y suscriptor de Cisco MediaSenseCisco SocialMinerEditor y suscriptor de Cisco UCCX

Para instalar los certificados autofirmados en la máquina del cliente, utilice a un administrador de la directiva o del paquete del grupo, o instalelos individualmente en el navegador de cada agente PC.

Para el Internet Explorer, instale los certificados autofirmados del client cara en el almacén de los **Trusted Root Certification Authority**.

Para el Mozilla Firefox, complete estos pasos:

1. Navegue a las **herramientas > a las opciones**.
2. Haga clic en la ficha Advanced (Opciones avanzadas).
3. Haga clic los **Certificados de la visión**.
4. Navegue a la lengueta de los **servidores**.
5. El tecleo **agrega la excepción**.

Integración y configuración del cliente

UCCX-a-MediaSense

El UCCX consume la interfaz de programación de aplicaciones del RESTO de los servicios web de MediaSense (API) para dos propósitos:

- Para inscribir a las notificaciones de las nuevas grabaciones que se invocan en el administrador de las Comunicaciones unificadas de Cisco (CUCM).
- Para marcar las grabaciones con etiqueta de los agentes UCCX con la información de la cola de servicios del agente y del contacto (CSQ).

El UCCX consume el RESTO API en los Nodos de la administración de MediaSense. Hay un máximo de dos en cualquier cluster de MediaSense. El UCCX no conecta vía el RESTO API con los Nodos de la extensión de MediaSense. Ambos Nodos UCCX deben consumir el RESTO API de MediaSense, así que instale los dos Certificados de MediaSense Tomcat en ambos Nodos UCCX.

Cargue el encadenamiento firmada o de certificado autofirmado de los servidores de MediaSense al keystore de la Tomcat-*confianza* UCCX.

MediaSense-a-delicadeza

MediaSense consume el RESTO API de los servicios web de la delicadeza para autenticar los agentes para el gadget de la búsqueda y del juego de MediaSense en la delicadeza.

El servidor de MediaSense configurado en la disposición de la delicadeza XML para el gadget de la búsqueda y del juego debe consumir el RESTO API de la delicadeza, así que instale los dos Certificados UCCX Tomcat en ese nodo de MediaSense.

Cargue el encadenamiento firmada o de certificado autofirmado de los servidores UCCX al keystore de la Tomcat-*confianza de* MediaSense.

UCCX-a-SocialMiner

El UCCX consume el RESTO y la notificación API de SocialMiner para manejar los contactos y la configuración del correo electrónico. Ambos Nodos UCCX se deben consumir el RESTO API de SocialMiner y notificar por el servicio de notificación de SocialMiner, así que instale el certificado de SocialMiner Tomcat en ambos Nodos UCCX.

Cargue el encadenamiento firmada o de certificado autofirmado del servidor de SocialMiner al keystore de la Tomcat-*confianza* UCCX.

Certificado del cliente del AppAdmin UCCX

El certificado del cliente del AppAdmin UCCX se utiliza para la administración del sistema UCCX. Para instalar el certificado del AppAdmin UCCX para los administradores UCCX, en PC del cliente, navegue a **https:// <UCCX FQDN>/appadmin/main** para cada uno de los Nodos UCCX y instale el certificado a través del navegador.

Certificado del cliente de la plataforma UCCX

Utilizan a los servicios web UCCX para la salida de los contactos de la charla a los buscadores del cliente. Para instalar el certificado de la plataforma UCCX para los agentes y los supervisores UCCX, en PC del cliente, navegue a **https:// <UCCX FQDN>/appadmin/main** para cada uno de los Nodos UCCX y instale el certificado a través del navegador.

Certificado del cliente del servicio de notificación

El CUIC utiliza al servicio de notificación CCX la delicadeza, el UCCX, y para enviar la información en tiempo real al escritorio del cliente vía la Mensajería y el protocolo extensibles de la presencia (XMPP). Esto se utiliza para la comunicación en tiempo real de la delicadeza así como CUIC viven los datos.

Para instalar el certificado del cliente del servicio de notificación en el PC de los agentes y de los supervisores o de los usuarios de la información que utilizan los datos vivos, navegan a **https:// <UCCX FQDN>:7443/** para cada uno de los Nodos UCCX y instalan el certificado a través del navegador.

Certificado del cliente de la delicadeza

El certificado del cliente de la delicadeza es utilizado por los escritorios de la delicadeza para conectar con Tomcat de la delicadeza el caso con el propósito de la comunicación del RESTO API entre el escritorio y el servidor de la delicadeza del coresidente.

Para instalar el certificado de la delicadeza para los agentes y los supervisores, en PC del cliente, navegar a **https:// <UCCX FQDN>:8445/** para cada uno de los Nodos UCCX y instalar el certificado con los prompts del navegador.

Para instalar el certificado de la delicadeza para los administradores de la delicadeza, en PC del cliente, navegar a **https:// <UCCX FQDN>:8445/cfadmin** para cada uno de los Nodos UCCX y instalar el certificado con los prompts del navegador.

Certificado del cliente de SocialMiner

El certificado de SocialMiner Tomcat se debe instalar en la máquina del cliente. Una vez que un agente valida una petición de la charla, el gadget de la charla se reorienta a un URL que represente la sala de chat. Esta sala de chat es recibida por el servidor de SocialMiner y contiene el cliente o el contacto de la charla.

Para instalar el certificado de SocialMiner en el navegador, en PC del cliente, navegar al **<SocialMiner FQDN>/de https://** y instalar el certificado con los prompts del navegador.

Certificado del cliente CUIC

El certificado CUIC Tomcat se debe instalar en la máquina del cliente para los agentes, los supervisores, y los usuarios de la información que utilizan la interfaz Web CUIC para los informes históricos o viven los datos señalan dentro de la página web CUIC o dentro de los gadgets en el escritorio.

Para instalar el certificado CUIC Tomcat en el navegador, en PC del cliente, navegar a **https://<UCCX FQDN>:8444/** y instalar el certificado con los prompts del navegador.

CUIC viven el certificado de los datos (desde 11.x)

El CUIC utiliza el servicio IO del socket para los datos vivos backend. Este certificado se debe instalar en la máquina del cliente para los agentes, los supervisores y los usuarios de la información que utilizan la interfaz Web CUIC para los datos Live o que utilizan los gadgets vivos de los datos dentro de la delicadeza.

Para instalar el certificado IO del socket en el navegador, en PC del cliente, navegar a **https://<UCCX FQDN>:12015/** y instalar el certificado con los prompts del navegador.

Aplicaciones de terceros accesibles de los scripts

Si un script UCCX se diseña para acceder una ubicación segura en un servidor de tercera persona (por ejemplo, *consiga el* paso del *documento URL a un* HTTPS URL o *haga la llamada del resto a un* RESTO URL HTTPS), cargue el encadenamiento firmada o de certificado autofirmado del servicio de otras compañías al keystore de la Tomcat-*confianza* UCCX. Para obtener este certificado, acceder la **página de administración** UCCX **OS** y elegir el **certificado de la carga**.

El motor UCCX se configura para buscar el keystore de Tomcat de la plataforma para las Cadenas de certificados de tercera persona cuando es presentado con estos Certificados por las aplicaciones de terceros cuando acceden las ubicaciones seguras vía los pasos del script.

La Cadena de certificados entera se debe cargar al keystore de Tomcat de la plataforma, accesible vía la **página de administración OS**, pues el keystore de Tomcat no contiene ningún certificado raíz por abandono.

Después de que usted complete estas acciones, recomience el motor de Cisco UCCX.

Verificación

Para verificar que todos los Certificados estén instalados correctamente, usted puede probar las características que se describen en esta sección. Si aparecen ningunos errores del certificado y funcionan todas las características correctamente, los Certificados están instalados correctamente.

- Configure la delicadeza de modo que registre automáticamente un agente vía el flujo de trabajo. Después de que una llamada sea manejada por el agente, utilice la aplicación de la búsqueda y del juego de MediaSense para encontrar la llamada. Verifique que la llamada tenga el agente, un CSQ, y etiquetas del equipo asociadas a los meta datos de la grabación en MediaSense.

- Configure la charla de la red del agente con SocialMiner. Inyecte un contacto de la charla vía la forma de la red. Verifique que el agente reciba el banner para validar el contacto de la charla y también para verificarlo que el contacto de la charla está validado una vez, las cargas de la forma de la charla correctamente y el agente puede recibir y enviar los mensajes de la charla.
- Tentativa de iniciar sesión un agente vía la delicadeza. Verifique que aparezcan ningunas advertencias del certificado y que la página web no indica para la instalación de los Certificados en el navegador. Verifique que el agente pueda cambiar los estados correctamente y una nueva llamada en UCCX está presentada correctamente al agente.
- Después de que usted configure los gadgets vivos de los datos en la disposición de escritorio de la delicadeza del agente y del supervisor, inicie sesión un agente, un supervisor, y a un usuario de la información. Verifique que los gadgets vivos de los datos carguen correctamente, que los datos iniciales están poblados en el gadget, y que los datos restauran cuando los datos subyacentes cambian.
- Intente conectar de un navegador con el AppAdmin URL en ambos Nodos UCCX. Verifique que aparezcan ningunas advertencias del certificado cuando estén indicadas con la página de registro.

Troubleshooting

Problema - Identificación del usuario/contraseña inválidas

Los agentes de la delicadeza UCCX no pueden iniciar sesión con el error “**identificación del usuario/contraseña inválidas**”.

Causas

CCX unificado lanza una excepción “SSLHandshakeException “y no puede establecer una conexión con el CM unificado.

Solución

- Verifique que no esté expirado el certificado unificado CM Tomcat.
- Asegúrese de que cualquier certificado que usted cargara en el CM unificado tenga de estas Extensiones marcadas como crítico:
  Uso de la clave X509v3 (OID - 2.5.29.15)
  Apremios básicos X509v3 (OID - 2.5.29.19)
  Si usted marca cualesquiera otras Extensiones como críticas, la comunicación falla entre CCX unificado y el CM unificado debido al error de verificación del certificado unificada CM.

Problema - El CSR SAN y certificado SAN no hace juego

La carga de un certificado firmado de CA visualiza el error “CSR SAN y el certificado SAN no hace juego”.

Causas

CA pudo haber agregado otro dominio del padre en el campo alternativo de los nombres del tema del certificado (SAN). Por abandono, el CSR tendrá éstos sin:

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

Los CA pudieron devolver un certificado con otro SAN agregado al certificado: www.hostname.example.com. El certificado tendrá un SAN adicional en este caso:

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

  www.hostname.example.com (dNSName)
]

Esto causa el error de la discordancía SAN.

Solución

En la sección del “nombre alterno sujeto (sin)” de la página del pedido de firma de certificado UCCX “genere”, generan el CSR con un campo vacío del dominio del padre. Esta manera el CSR no se genera con un atributo SAN, CA puede formatar sin, y no habrá una discordancía del atributo SAN cuando usted carga el certificado a UCCX. Observe que el campo del dominio del padre omite el dominio del servidor UCCX, así que el valor debe ser quitado explícitamente mientras que las configuraciones para el CSR se configuran.

Problema - RED:: ERR_CERT_COMMON_NAME_INVALID

Cuando usted accede cualquier página web UCCX, de MediaSense, o de SocialMiner, usted recibe un mensaje de error.

“Su conexión no es privada.

Los atacantes pudieron intentar robar su información del <Server_FQDN> (por ejemplo, las contraseñas, los mensajes, o las placas de crédito). RED:: ERR_CERT_COMMON_NAME_INVALID

Este servidor no podría probar que es <Server_FQDN>; su Security Certificate es de [missing_subjectAltName]. Esto se puede causar por un misconfiguration o un atacante que intercepta su conexión.”

Causas

La versión 58 de Chrome introdujo una nueva función de seguridad donde señala que el certificado de un sitio web no es seguro si su Common Name (CN) también no se incluye como SAN.

Solución

- Usted puede navegar a **avanzado > procede al <Server_FQDN> (inseguro)** para continuar al sitio y validar el error del certificado.
- Usted puede evitar el error en conjunto con los certificados firmados de CA. Cuando usted genera un CSR, el FQDN del servidor se incluye como SAN. CA puede firmar el CSR, y después de que usted cargue el certificado firmado de nuevo al servidor, el certificado de servidor tendrá el FQDN en el campo SAN de modo que el error no sea presentado.

Más información

Vea la sección “quitar el soporte para el commonName que corresponde con en los Certificados” en las deprecaciones y los retiros en Chrome 58.

Certifique los defectos

- Id. de bug Cisco CSCvb46250 - UCCX: Impacto del certificado de Tomcat ECDSA en los datos vivos de la delicadeza
- Id. de bug Cisco CSCvb58580 - Incapaz de iniciar sesión a SocialMiner con ambo tomcat y a Tomcat-ECDSA firmó por RSA CA
- Id. de bug Cisco CSCvd56174 - UCCX: Error en el inicio de sesión del agente de la delicadeza debido a SSLHandshakeException
- Id. de bug Cisco CSCuv89545 - Vulnerabilidad del amontonamiento de la delicadeza

Información Relacionada

- Entienda los Certificados ECDSA en una solución UCCX
- UCCX firmado y ejemplo de configuración de los certificados autofirmados
- Soporte Técnico y Documentación - Cisco Systems