Guía de Cómo completa del Jabber para la validación de certificado

Contenido

Introducción

Este documento combina a varios recursos de Cisco en un completo, unificado cómo-a la guía que se utiliza para implementar todos los requisitos para la validación de certificado en el Jabber de Cisco. Esto es necesario porque el Jabber de Cisco ahora requiere el uso de la validación de certificado para establecer las conexiones seguras con los servidores. Este requisito exige muchos cambios que se pudieron requerir para los entornos del usuario.

> Nota: Esta guía está para las implementaciones de la en-premisa solamente. No hay actualmente cambio requerido para las instrumentaciones del servicio de la nube, porque se validan contra el Certificate Authority (CA) público.

¿Este cambio afectan a qué clientes del Jabber?

Aquí está una tabla que enumera a todos los clientes que implementen la validación de certificado:

Tabla 1

Clientes de escritorio	Clientes del móvil y de la tablilla
Jabber para la versión 9.2 (septiembre de 2013) de Macintosh Jabber para la versión de Windows 9.2.5 (septiembre de 2013) de Microsoft (MS)	Jabber para la versión 9.5 (octubre de 2013) iPhone Jabber para la versión 9.6 (noviembre de 20 del iPhone y del iPad Jabber para la versión 9.6 (diciembre de 201 Android

¿Qué hace este medio para el entorno del Jabber?

Cuando usted instala o actualización a cualquier cliente enumerado en el **cuadro 1**, la validación de certificado obligatoria con los servidores se utiliza para las conexiones seguras. Esencialmente, cuando los clientes del Jabber intentan ahora hacer una conexión segura, actual Jabber de Cisco de los servidores con los Certificados. El Jabber de Cisco entonces intenta validar esos Certificados contra el almacén de certificados del dispositivo. Si el cliente no puede validar el certificado, le indica a que confirme que usted quiera validar el certificado, y lo coloque en su almacén de la confianza de la empresa.

¿Se requieren qué Certificados?

Aquí está una lista de servidores de la en-premisa y los Certificados que presentan a Cisco el Jabber para establecer una conexión segura:

Tabla 2

Servidor	Certificado
Cisco Unified Presence	HTTP (Tomcat) XMPP
Administrador de las Comunicaciones unificadas de Cisco IM y presencia	HTTP (Tomcat) XMPP
Administrador de las Comunicaciones unificadas de Cisco	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)
Servidor de las reuniones del WebEx de Cisco	HTTP (Tomcat)

Aquí están algunos puntos importantes a observar:

- Aplique la actualización más reciente del servicio (SU) para el Cisco Unified Presence (TAZA) o el administrador de las Comunicaciones unificadas de Cisco (CUCM) IM y presencia antes de que usted comience el proceso de firma del certificado.
- Los Certificados requeridos se aplican a todas las versiones del servidor. Por ejemplo, versión 8.x de la TAZA y CUCM IM y presente de la versión 9.x y posterior de la presencia el cliente con la Mensajería y el protocolo de la presencia (XMPP) y los Certificados extensibles HTTP.
- Cada nodo en un cluster, los suscriptores y los editores, funciona con un servicio de Tomcat y puede presentar al cliente con un certificado HTTP. Planee firmar los Certificados para cada nodo en el cluster.
- Para asegurar el Session Initiation Protocol (SIP) que señala entre el cliente y el CUCM, utilice la inscripción de la función de proxy de las autoridades de certificación (CAPF).

¿Qué métodos están disponibles para la validación de certificado?

Hay actualmente varios métodos de validación de la certificación que pueden ser utilizados.

Método 1: El tecleo de los usuarios **valida** simplemente a todo el popups del certificado. Ésta pudo ser la mayoría de la solución ideal para entornos más pequeños. Si usted tecleo **valida**, los Certificados se colocan en el almacén de la confianza de la empresa en el dispositivo. Después de que los Certificados se coloquen en el almacén de la confianza de la empresa, indican a los usuarios no más cuando registran en el cliente del Jabber en ese dispositivo local.

Método 2: Los Certificados requeridos (el **cuadro 2)** se descarga de los servidores individuales (por abandono, éstos son certificados autofirmados) y está instalado en el almacén de la confianza de la empresa del dispositivo del usuario. Ésta pudo ser la solución ideal si su entorno no tiene acceso a un Privado o público CA para la firma del certificado.

Varios métodos se pueden utilizar para avanzar estos Certificados a los usuarios, pero un método rápido es emplear el uso del registro de Microsoft Windows:

1. A partir de la una de las máquinas, valide todos los Certificados que se presenten para farfullar en el almacén de la confianza de la empresa.
2. Para verificar que los Certificados estén presentes, ingresen el **comando Certmgr.msc** y naveguen a EnterpriseTrust **> a los Certificados.**
3. Abra **Regedit** con un comando del **funcionamiento** y navegue a **HKCU > software > Microsoft > SystemCertificates > confianza > los Certificados**.
4. Haga clic con el botón derecho del ratón y exporte la carpeta de Certifates en el registro como un archivo **.reg**.
5. Elimine este archivo vía el objeto de la directiva del grupo (GPO) a todos los usuarios (o al otro método preferido).

Esto completa el instalar de los Certificados de confianza de la empresa para el Jabber, y indican a los usuarios no más.

Método 3: Un público o un soldado CA (el **cuadro 2)** firma todos los Certificados requeridos. Éste es el método recomendado de Cisco. Este método requiere que un pedido de firma de certificado (CSR) esté generado para cada uno de los Certificados, se firma, re-está cargado al servidor, y después importado a las autoridades de certificación de la Raíz confiable el almacén en los dispositivos del usuario. ¿Vea la **generación un CSR** y **cómo llego los Certificados a los almacenes de certificados de los dispositivos del usuario?** secciones de este documento para más información.

> Nota: En el caso de CA público, el certificado raíz debe ya estar en el almacén de la confianza del cliente.

Es importante recordar que el público CA requiere típicamente los CSR para ajustarse a los formatos específicos. Por ejemplo, CA público pudo validar solamente los CSR eso:

- Sea codificado en base64
- ¡No contenga ciertos caracteres, tales como @&! , en la organización, la unidad organizativa (OU), u otros campos

- Utilice las longitudes de bit específicas en la clave pública para el servidor

Asimismo, si usted somete los CSR de los nodos múltiples, el público CA pudo requerir que la información sea constante en todos los CSR.

Para prevenir los problemas con sus CSR, revise los requisitos del formato de CA público a las cuales usted planea someter los CSR. Entonces asegúrese de que la información que usted ingresa cuando usted configura su servidor se ajusta al formato que el público CA requiere.

Aquí está un requisito posible que usted puede ser que encuentre:

Un certificado por el FQDN: Una cierta muestra del público CA solamente un certificado por el nombre de dominio completo (FQDN).

Por ejemplo, para firmar los Certificados HTTP y XMPP para un solo CUCM IM y el nodo de la presencia, usted puede ser que necesite someter cada CSR a diverso público CA.

Verifique si Uno mismo-se firma o CA-se firma un certificado

> Nota: Este ejemplo está para la versión 8.x CUCM. El proceso pudo variar entre los servidores.

1. Navegue a **Cisco unificó la administración OS**.
2. Elija el **Certificate Management (Administración de certificados) de la Seguridad**.
3. Encuentre y haga clic el archivo del **.pem del certificado de la Tomcat-confianza**.
4. Haga clic la **descarga**, y **sálvela**.
5. Navegue al archivo, y retitúlelo con la extensión de **.cer**.
6. Abra y vea este archivo (usuarios de MS Windows).
7. Verifique **publicado por el** campo. Si hace juego **publicado** para colocar, después Uno mismo-se firma el certificado (véase el **ejemplo**).

Ejemplo: Uno mismo-firmado contra el soldado certificado firmado por CA

Soldado Uno mismo-firmado CA-firmado

Genere un CSR

> Nota: Este ejemplo está para la versión 8.x CUCM. El proceso pudo variar entre los servidores.

1. Navegue a **Cisco unificó la administración OS**.
2. Elija el **Certificate Management (Administración de certificados) de la Seguridad**.
3. El tecleo **genera el CSR**, y elige **Tomcat de la** lista desplegable.
4. El tecleo **genera el CSR**, y hace clic **cerca**.
5. Haga clic la **descarga CSR**, y elija **Tomcat de la** lista desplegable.
6. Haga clic la **descarga CSR**, y salve el archivo.
7. Envíe el archivo **.csr** que se firmará por su servidor privado de CA o CA público.
   Nota: Una vez que usted tiene este archivo CSR, el proceso varía basado en su entorno.

8. Haga clic el **certificado/la Cadena de certificados de la carga** bajo re-carga del **Certificate Management (Administración de certificados) de la Seguridad** para los nuevos certificados firmados que fueron publicados a su servidor.

¿Cómo hacen los Certificados de importación I en los almacenes de certificados del dispositivo del usuario?

Cada certificado de servidor debe tener un certificado raíz asociado presente en el almacén de la confianza en el dispositivo del usuario. El Jabber de Cisco valida los Certificados que los servidores presentes contra los certificados raíz en la confianza salvan.

Importe los certificados raíz en el almacén de certificados de MS Windows si:

- Los Certificados son firmados por CA que no existe ya en el almacén de la confianza, tal como un soldado CA si es así usted debe importar el certificado de CA privado al almacén de los Trusted Root Certification Authority.
- Uno mismo-se firman los Certificados. Si es así usted debe importar los certificados autofirmados al almacén de la confianza de la empresa.

Usted puede utilizar cualquier Certificados de importación del método adecuado para en el almacén de certificados de MS Windows, por ejemplo:

- Utilice los Certificados de importación del Asisitente de la importación del certificado para individualmente.
- Despliegue los Certificados a los usuarios con la herramienta de la línea de comando CertMgr.exe en el servidor de MS Windows. (Esta opción le requiere utilizar la herramienta del Certificate Manager, CertMgr.exe, no la consola de administración de los Certificados MS, CertMgr.msc.)
- Despliegue los Certificados a los usuarios con un GPO en el servidor de MS Windows.

  Nota: Para las Instrucciones detalladas en cómo a los Certificados de importación, refiera a la documentación apropiada MS.

Identidad del servidor en los Certificados

Como parte del proceso de firma, CA especifica la identidad del servidor en el certificado. Cuando el cliente valida ese certificado, marca eso:

- Una autoridad de confianza ha publicado el certificado.
- La identidad del servidor que presenta el certificado hace juego la identidad del servidor especificada en el certificado.

  Nota: El público CA requiere generalmente un FQDN como la identidad del servidor, no una dirección IP.

Campos del identificador

El cliente marca estos campos del identificador en los certificados de servidor para una coincidencia de la identidad:

Certificados XMPP

- SubjectAltName \ OtherName \ xmppAddr
- SubjectAltName \ OtherName \ srvName
- SubjectAltName \ dnsNames
- Tema CN

Certificados HTTP

- SubjectAltName \ dnsNames
- Tema CN

Nota: El campo del tema CN puede contener a un comodín (*) como el carácter de izquierda; por ejemplo, *.cisco.com. Su CUCM, TAZA, y servidores del Cisco Unity Connection no pudieron soportar los Certificados del comodín. (Refiera al Id. de bug Cisco CSCta14114 de la mejora).

Prevenga la discordancía de la identidad

Cuando un cliente del Jabber intenta conectar con un servidor con una dirección IP, y el certificado de servidor identifica el servidor con un FQDN, el cliente no puede identificar el servidor según lo confiado en y indica al usuario. Así pues, si sus certificados de servidor identifican los servidores con los FQDN, usted debe especificar Nombre del servidor como FQDN en muchos lugares en sus servidores.

El cuadro 3 enumera todos los lugares que necesiten especificar Nombre del servidor mientras que aparece en el certificado, si es una dirección IP o un FQDN.

Cuadro 3

Servidor	Ubicación (la configuración debe hacer juego el certificado)
Clientes del Jabber de Cisco	Dirección del servidor del login (diferencia para los clientes, normalmente bajo **configuraciones de la conexión)** ** Todos los Nombres del nodo (**sistema > topología de clústers)** ** **Precaución**: ¡Aseegurese que si usted cambia esto al FQDN, usted puede resol esto vía el DNS o los servidores permanecen en el estado que comienza! Servidores TFTP (**aplicación > Jabber > configuraciones de Cisco)**
TAZA (versión 8.x y anterior)	Cisco IP Phone primario y secundario del Cisco Call Manager (CCMCIP) (**aplicaci Jabber de Cisco > perfil CCMCIP)** Nombre del host del voicemail (**aplicación > Jabber > servidor de correo de voz de Cisco)** Nombre del mailstore **(aplicación > Jabber > mailstore de Cisco)** Nombre del host de la Conferencia (**aplicación > servidor del Jabber > de la Conferencia de Cisco)** (Meeting Place (Lugar de encuentro) solamente) Dominio XMPP (véase el **dominio del proporcionar XMPP a la** sección de los **clien**
CUCM IM y presencia	** Todos los Nombres del nodo **(sistema > topología de clústers**)

(versión 9.x y posterior)	** **Precaución**: ¡Aseegurese que si usted cambia esto al FQDN, usted puede resol esto vía el DNS o los servidores permanecen en el estado que comienza! Servidores TFTP (**aplicación > clientes > configuraciones de la herencia)** CCMCIP primario y secundario **(aplicación > clientes de la herencia > perfil CCMC** Dominio XMPP (véase el **dominio del proporcionar XMPP a la** sección de los **clien**
CUCM (versión 8.x y anterior)	Nombre del servidor (**System (Sistema) > Server (Servidor))**
CUCM (versión 9.x y posterior)	Nombre del servidor **(System (Sistema) > Server (Servidor))** IM y servidor de la presencia (**User Management (Administración de usuario) > aju de usuario > servicio UC > IM y presencia)** Nombre del host del voicemail **(User Management (Administración de usuario) > a de usuario > servicio > voicemail UC)** Nombre del mailstore **(User Management (Administración de usuario) > ajustes de usuario > servicio > mailstore UC)** Nombre del host de la Conferencia (**(User Management (Administración de usuario ajustes de usuario > servicio > Conferencia UC)** (Meeting Place (Lugar de encuen solamente)
Cisco Unity Connection (todas las versiones)	**Ningún cambio necesario**

Proporcione el dominio XMPP a los clientes

El cliente identifica los Certificados XMPP con el dominio XMPP, bastante que con el FQDN. Los Certificados XMPP deben contener el dominio XMPP en un campo del identificador.

Cuando el cliente intenta conectar con el servidor de la presencia, el servidor de la presencia proporciona el dominio XMPP al cliente. El cliente puede entonces validar la identidad del servidor de la presencia contra el certificado XMPP.

Complete estos pasos para asegurarse de que el servidor de la presencia proporciona el dominio XMPP al cliente:

1. Abra la interfaz de la administración para su servidor de la presencia, **Cisco unificó CM IM y la interfaz de la administración de la presencia** o la **interfaz de la administración del Cisco Unified Presence**.
2. Navegue al **> Security (Seguridad) > a las configuraciones del sistema**.
3. Localice la sección de las **configuraciones del certificado XMPP**.
4. Especifique el dominio del servidor de la presencia en el **Domain Name para el campo de nombre de la alternativa del tema del certificado del Servidor-a-servidor XMPP**.
5. Marque el **Domain Name del uso para la** casilla de verificación **alternativa del nombre del tema del certificado XMPP**.
6. Haga clic en Save (Guardar).
7. Después de que usted salve este cambio, usted debe regenerar el certificado de la **taza-xmpp** en el servidor.
8. Recomience al **router XCP** para que el cambio tome el efecto.

   Precaución: Un reinicio del router XCP afecta el servicio.

¡La validación de certificado es completa ahora!

Información Relacionada

- Jabber de Cisco 9.2.5 Release Note
- Jabber de Cisco: Nota Técnica obligatoria de la validación del certificado de servidor
- Soporte Técnico y Documentación - Cisco Systems