El Troubleshooting Cisco unificó el gadget del centro de la inteligencia (CUIC) sobre el HTTPS en la delicadeza

Contenido

Introducción
Problema
Solución
Paso 1. Descargue el certificado tomcat.pem del host de tercera persona del gadget.
Paso 2. Cargue el certificado al servidor primario de la delicadeza.
Paso 3. Recomience la delicadeza Tomcat de Cisco en el servidor primario de la delicadeza.
Paso 4. Después de que la sincronización sea completa, recomience la delicadeza Tomcat de Cisco en el secundario
    Servidor de la delicadeza.
Otro problema
Solución
Paso 1. De la página de administración de la plataforma en la delicadeza, certificado del tomcat de la carga CUIC como Tomcat-confianza
Paso 2. Certificados de la delicadeza de la carga a CUIC como Tomcat-confianza
Paso 3. Recomience éstos en el editor y suscriptor de la delicadeza durante la ventana de mantenimiento con
    estos comandos
Paso 4. Restat estos servicios en el editor y suscriptor CUIC

Introducción

Este documento describe cómo resolver problemas el gadget CUIC (centro unificado Cisco de la inteligencia) en la delicadeza de Cisco sobre HTTS. Este problema fue encontrado durante el impletementation del gadget.

Contribuido por Sahar Modares, ingeniero de Cisco TAC.

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

CUIC

Finesse

Componente usado

CUIC 10.5

Delicadeza 11.0

Problema

El nuevo gadget CUIC fue creado con este link, en la disposición admin de la delicadeza:

<gadget>/3rdpartygadget/files/WebService/WebService.xml</gadget>

Pero, falló con este mensaje de error:

“Estatus 500 HTTP - javax.net.ssl.SSLPeerUnverifiedException: par no autenticado”

Solución

La comunicación HTTPS se debe permitir entre el envase del gadget de la delicadeza y el sitio de tercera persona del gadget para cargar el gadget y realizar cualquier llamada API que el gadget haga al servidor de tercera persona.

El certificado se debe firmar con un Common Name. El gadget URL en la disposición de escritorio debe utilizar el mismo nombre (si utiliza una dirección IP o un Nombre de dominio totalmente calificado (FQDN)) mientras que el nombre con el cual se firma el certificado. Si el nombre del certificado y el nombre en el gadget URL no hace juego, la conexión no se confía en y el gadget no carga.

Para encontrar el nombre del certificado, ingrese el gadget URL en su hojeador. Haga clic el icono del bloqueo en la barra de dirección y después haga clic los detalles de la visión. Busque el campo del Common Name.

El host de la delicadeza debe poder resolver este nombre usando el host DNS que fue ingresado durante la instalación. Para verificar que la delicadeza pueda resolver el nombre, funcione con el comando CLI “<hostname> del ping de la red del utils”.

Paso 1. Descargue el certificado tomcat.pem del host de tercera persona del gadget.

1. a) Ingrese a Cisco unificó la administración del sistema operativo en el host de tercera persona del gadget (https:// *FQDN/cmplatform*, donde está el Nombre de dominio totalmente calificado (FQDN) el *FQDN del* host de tercera persona del gadget).
2. b) Haga clic Security>CertificateManagement.
3. c) Haga clic en Find (Buscar).
4. d) Haga clic tomcat.pem.
5. e) Haga clic la descarga y salve el archivo en su escritorio.

Paso 2. Cargue el certificado al servidor primario de la delicadeza.

1. a) Ingrese a Cisco unificó la administración del sistema operativo en el servidor primario de la delicadeza (http:// *FQDN:8080/cmplatform*, donde está el Nombre de dominio totalmente calificado (FQDN) el *FQDN del* servidor de la delicadeza).
2. b) Haga clic Security>CertificateManagement.
3. c) Haga clic el certificado de la carga.

4. d) FromtheCertificateNamedrop-downlist, Tomcat-confianza selecta.
5. e) Haga clic hojean y navegan al archivo tomcat.pem que usted descargó en el paso anterior.

1. f) Haga clic el archivo de la carga.

Paso 3. Recomience la delicadeza Tomcat de Cisco en el servidor primario de la delicadeza.

Paso 4. Después de que la sincronización sea completa, recomience la delicadeza Tomcat de Cisco en el secundario

Servidor de la delicadeza.

Otro problema

Una vez que usted carga el certificado de tercera persona que en este caso es CUIC a la delicadeza, usted espera ver que el gadget esté cargado a la delicadeza, pero todavía falla con el mensaje de error mencionado en la sección de problemas.

Solución

El error “javax.net.ssl.SSLPeerUnverifiedException: solucionaron al par no autenticado” con los siguientes pasos:

Paso 1. De la página de administración de la plataforma en la delicadeza, certificado del tomcat de la carga CUIC como Tomcat-confianza

Paso 2. Certificados de la delicadeza de la carga a CUIC como Tomcat-confianza

Paso 3. Recomience éstos en el editor y suscriptor de la delicadeza durante la ventana de mantenimiento con

estos comandos

- reinicio Cisco Tomcat del servicio del utils
- delicadeza Tomcat de Cisco del reinicio del servicio del utils

Paso 4. Restat estos servicios en el editor y suscriptor CUIC

- reinicio Cisco Tomcat del servicio del utils

- servicio de la información del centro de la inteligencia del reinicio del servicio del utils