El alcance de este documento es un recorrido simple en configurar el SSL en el Cisco Intelligent Automation for Cloud. Esta configuración utilizará los certificados autofirmados pero se puede utilizar con los Certificados de tercera persona o de la Raíz confiable. Esto no es un reemplazo para ninguna documentación SSL en la cartera de la documentación IAC.

- Configurar el SSL en el servidor del catálogo del servicio
- Configurar el SSL en el servidor de proceso del Orchestrator
- Configurar el catálogo de proceso del Orchestrator y del servicio para utilizar el SSL con uno a
- Configurando RequestCenter y ServiceLink para utilizar el SSL para comunicar (opcional)

El servidor del catálogo del servicio consiste en dos componentes que sean configurados para el SSL: RequestCenter y ServiceLink. Esta configuración fue hecha en una configuración de JBoss del dos-servidor pero debe trabajar en una configuración de JBoss del uno-servidor también. Esta configuración trabajará en Windows o un servidor del catálogo del servicio de Linux. Los pasos mostrarán la configuración en un servidor del catálogo del servicio de Windows pero se pueden utilizar en un servidor del catálogo del servicio de Linux. En los pasos debajo del **<JBOSS_RC_HOME>** variable refiere al directorio de inicio de JBoss para RequestCenter, **<JBOSS_SL_HOME>** refiere al directorio de inicio de JBoss para ServiceLink, y **<JAVA_HOME>** refiere al directorio de inicio de las Javas.
Esta sección contiene los temas siguientes:

- Configurar el SSL en RequestCenter
- Configurar el SSL en ServiceLink

Configurar el SSL en RequestCenter

Esta sección contiene los temas siguientes:

- Cree el certificado
- Certificado de exportación
- Import Certificate (Importar certificado) al almacén de la confianza de JBoss
- Import Certificate (Importar certificado) en el almacén de la confianza de las Javas
- Edite el archivo de configuración standalone-full.xml

Cree el certificado

La primera cosa a hacer es crear un certificado autofirmado.

1. Abra un comando prompt.
2. Cambie los directorios a **<JBOSS_RC_HOME> \ a RequestCenterServer \ a la configuración**.
3. Cree un certificado autofirmado funcionando con el comando **<JAVA_HOME> \ jre \ compartimiento \ keytool - genkey - alias alias> del <requestcenter - el keyalg RSA - password> de los <keypass de los keypass - password> de los <storepass de los storepass - el keystore keystore.jks**

   Con el propósito de la configuración el alias usado es **RequestCenter** y los keypass y la

contraseña de los storepass es el **changeit de la** contraseña predeterminada.

NOTA: A le indicarán que ingrese la información sobre este certificado. El primer prompt es **cuál es su nombre y apellido** (también llamado el CN). Éste debe ser el nombre del host de la máquina o del **localhost**. El resto de la información puede ser sea cual sea usted quiere introducir.

Certificado de exportación

La cosa siguiente a hacer es exportar el certificado a un archivo.

1. Abra un comando prompt.
2. Cambie los directorios a **<JBOSS_RC_HOME> \ a RequestCenterServer \ a la configuración**.
3. Exporte el certificado a un archivo funcionando con el comando **<JAVA_HOME> \ jre \ compartimiento \ keytool - exportación - alias alias> del <requestcenter - password> de los <storepass de los storepass - clasifían el nombre del archivo del certificado del <requestcenter > - el keystore keystore.jks**

   Con el propósito de la configuración el nombre del archivo usado es **RequestCenter.cer**.

Import Certificate (Importar certificado) al almacén de la confianza de JBoss

La cosa siguiente a hacer es importar el certificado en el almacén de la confianza de JBoss.

1. Abra un comando prompt.
2. Cambie los directorios a **<JBOSS_RC_HOME> \ a RequestCenterServer \ a la configuración**.
3. Importe el certificado en el almacén de la confianza de JBoss funcionando con el comando **<JAVA_HOME> \ jre \ compartimiento \ keytool - importación - v - los trustcacerts - alias alias> del <requestcenter - clasifíe el nombre del archivo del certificado del <requestcenter > - el keystore cacerts.jks - password> de los <keypass de los keypass - password> de los <storepass de los storepass.**

Import Certificate (Importar certificado) en el almacén de la confianza de las Javas

La cosa siguiente a hacer es importar el certificado en el almacén de la confianza de las Javas.

1. Abra un comando prompt.
2. Cambie los directorios a **<JAVA_HOME> \ al jre \ a la liberación \ a la Seguridad**.
3. Copie el archivo de certificado de RequestCenter de <JBOSS_RC_HOME> \ de RequestCenterServer \ de la configuración en este directorio.
4. Importe el certificado en el almacén de la confianza de las Javas funcionando con el comando **<JAVA_HOME> \ jre \ compartimiento \ keytool - importación - v - los trustcacerts - alias alias> del <requestcenter - clasifíe el nombre del archivo del certificado del <requestcenter > - los cacerts del keystore - password> de los <keypass de los keypass - password> de los <storepass de los storepass**.

Edite el archivo de configuración standalone-full.xml

La cosa siguiente a hacer es editar el archivo de configuración standalone-full.xml.

1. Abra el archivo **<JBOSS_RC_HOME> \ RequestCenterServer \ configuración \ standalone-full.xml con un** editor de textos apropiado.
2. Busque para el **socket-binding= " HTTP”/> del scheme= " HTTP” del name= " HTTP” el protocol="HTTP/1.1" del <connector** y agregue las siguientes líneas después de él:

   secure= " del " https del socket-binding=” del " https” del scheme= del " https” del name= del <connector el protocol="HTTP/1.1" verdad " >
   certificate-key-file= " <JBOSS_RC_HOME> \ RequestCenterServer \ configuración \ keystore.jks”/> del " changeit” del password= alias>” del <requestcenter del key-alias= del " del <ssl
   </connector>

   NOTA: Alias> del <requestcenter del cambio al RequestCenter alias que usted está utilizando y que **<JBOSS_RC_HOME> al** directorio de inicio de JBoss para RequestCenter.
3. Salve el archivo **standalone-full.xml.**
4. Recomience RequestCenter.

Configurar el SSL en ServiceLink

Para configurar el SSL en ServiceLink, relance los pasos en el SSL que configura en la sección de RequestCenter del documento, aseegurandose le utilizar el directorio **<JBOSS_SL_HOME>** y el alias> del <servicelink.

Configurar el SSL en el servidor de proceso del Orchestrator

El servidor de proceso del Orchestrator es un Servidor Windows que utiliza el IIS. Esta sección contiene los temas siguientes:

- Cree el certificado
- Certificado de exportación
- Certificado del lazo para procesar el puerto SSL del Orchestrator

Cree el certificado

La primera cosa a hacer es crear un certificado autofirmado.

1. Abra al Administrador IIS.
2. En el lado izquierdo de la ventana, seleccione el servidor de proceso del Orchestrator.
3. A la derecha de la ventana, haga doble clic en los certificados de servidor.
4. En el lado derecho lejano de las ventanas de los certificados de servidor, haga clic en crean el certificado autofirmado.
5. Ingrese un nombre cómodo para el certificado y haga clic la AUTORIZACIÓN.

Certificado de exportación

1. Después de que se cree el certificado, haga clic con el botón derecho del ratón en él y seleccione la visión.
2. Haga clic en la lengueta de los detalles y haga clic en la copia para clasifiar
3. En el Asisitente de la exportación del certificado haga clic **después**.
4. Selecto **"no, no exporta la clave privada"** y hace clic **después**.
5. Seleccione **x.509 codificado base 64 (.CER)** y haga clic **después**.
6. Ingrese un nombre del archivo y haga clic **después**.
7. Clic en Finalizar para salvar el archivo de certificado.

Certificado del lazo para procesar el puerto SSL del Orchestrator

1. Abra el archivo de certificado, haga clic en la lengueta de los detalles, y navegue hacia abajo a Thumbprint en la sección del campo de la copia de cuadro de los detalles el valor hex para Thumbprint - éste es el valor de troceo del certificado.
2. Abra un comando prompt.
3. Funcione con HTTP del netsh del comando "agregan el certhash=<thumbprint> el appid={1776a671-8e9c-45b0-8304-dec6f472131f}" del sslcert ipport=0.0.0.0:61526

   El ipport=0.0.0.0:61526 es la dirección IP y el puerto SSL para el Orchestrator de proceso. Debe ser 0.0.0.0:61526.

   El certhash es el valor de Thumbprint que usted copió en el paso 1.

   *NOTE: Usted debe quitar los espacios en el valor de Thumbprint. El appid es siempre {1776a671-8e9c-45b0-8304-dec6f472131f}.

Configurar el catálogo de proceso del Orchestrator y del servicio para utilizar el SSL con uno a

Ahora que el SSL se configura en el catálogo del servicio y el Orchestrator del proceso, estos servidores necesitan ser configurados para comunicar con uno a usando el SSL. Para hacer que los servidores necesitan confiarse en. Eso es hecha agregando los archivos de certificado de servidor en el almacén de la confianza. Esta sección contiene los temas siguientes:

- Agregar los Certificados del catálogo del servicio al almacén de proceso de la confianza del Orchestrator
- Agregar los Certificados del Orchestrator del proceso al almacén de la confianza del catálogo del servicio
- Configurar el servidor de proceso del Orchestrator para utilizar el SSL
- Configure los agentes de RequestCenter para utilizar el SSL

Agregar los Certificados del catálogo del servicio al almacén de proceso de la confianza del Orchestrator

El servidor de proceso del Orchestrator necesita tener los Certificados del servidor del catálogo del servicio (los Certificados de RequestCenter y de ServiceLink) instalado en su almacén de la confianza.

1. Copie los archivos de certificado de RequestCenter y de ServiceLink sobre el servidor de proceso del Orchestrator.
2. Haga clic con el botón derecho del ratón en el archivo de certificado de RequestCenter y seleccione “instalan el certificado”.
3. En la ventana del Asistente de la importación del certificado haga clic después.
4. Seleccione el “lugar todos los Certificados en el almacén siguiente” y el tecleo hojea.
5. Seleccione los “Trusted Root Certification Authority” y haga clic la AUTORIZACIÓN.
6. Haga clic después
7. Clic en Finalizar para completar la instalación del certificado.
8. Un mensaje de error puede surgir con respecto al certificado que la demanda es de “localhost”. Este error es aceptable. Haga clic sí para instalar el certificado.
9. En la ventana más reciente, haga clic la AUTORIZACIÓN para completar el proceso de instalación.
10. Relance los pasos 2-9 para instalar el certificado de ServiceLink.

Agregar los Certificados del Orchestrator del proceso al almacén de la confianza del catálogo del servicio

El servidor del catálogo del servicio necesita tener el certificado del servidor de proceso del Orchestrator instalado en su almacén de la confianza.

1. Abra un comando prompt.
2. Cambie los directorios a <JAVA_HOME> \ al jre \ a la liberación \ a la Seguridad.
3. Copie el archivo de certificado de proceso del Orchestrator al servidor del catálogo del servicio en el directorio <JAVA_HOME> \ del jre \ de la liberación \ de la Seguridad.
4. Importe el certificado en el almacén de la confianza de las Javas funcionando con el comando **<JAVA_HOME> \ jre \ compartimiento \ keytool - importación - v - los trustcacerts - alias alias> del Orchestrator del <process - clasifíe el nombre del archivo del certificado del Orchestrator del <process > - los cacerts del keystore - password> de los <keypass de los keypass - password> de los <storepass de los storepass**.
5. Recomience RequestCenter y ServiceLink.

Configurar el servidor de proceso del Orchestrator para utilizar el SSL

El servidor de proceso del Orchestrator necesita ser configurado para utilizar el SSL. Las propiedades del servidor y las diversas blancos necesitan ser configuradas para utilizar el SSL. Esta sección contiene los temas siguientes:

- Cambie las propiedades del servidor (las propiedades del entorno)
- Configure las blancos

Cambie las propiedades del servidor (las propiedades del entorno)

1. Ábrase y registre en la consola de proceso del Orchestrator.
2. Del menú de archivos, seleccione las propiedades del servidor (propiedades del entorno en IAC 4.0).
3. Seleccione la lengueta del servicio web
4. No reelija como candidato el “servicio web NON-seguro del permiso (HTTP)” y seleccione el “servicio web seguro del permiso (HTTPS)”. Usted puede ver el siguiente mensaje:

   Habilitar los servicios web de proceso del Orchestrator de Cisco en un puerto seguro (HTTPS) requiere la configuración manual adicional. Refiera por favor a los documentos para obtener instrucciones.

   Haga Click en OK en este mensaje.
5. Usted puede seleccionar un puerto HTTPS pero el valor por defecto de 61526 debe ser aceptable.
6. Haga clic “restauran el servicio de red” y después hacen clic en OK.

Configure las blancos

Las blancos “integración porta API de la nube de Cisco”, “centro porta API de la petición de la nube de Cisco”, “servicio web de proceso del Orchestrator de Cisco”, y “servidor de portal de los servicios de Cisco” toda la necesidad de ser configurado para utilizar el HTTPS y el puerto SSL.

1. En la consola de proceso del Orchestrator, a la izquierda la parte del extremo inferior izquierdo las definiciones selectas de la ventana, por la parte de la superior izquierda las blancos selectas de la ventana, y a la derecha del clic doble de la ventana en “Cisco la blanco de la integración nube API porta”.
2. Haga clic en el cambio de la lengueta de la conexión la base URL a:

   hostname> del <cp de https://: <ServiceLink SSL port>/IntegrationServer/services

   donde está el hostname> del <cp el nombre de host o la dirección IP del port> del servidor y del <ServiceLink SSL del catálogo del servicio es el puerto SSL de ServiceLink. El puerto predeterminado es 6443.
3. Haga Click en OK para salvar los cambios.
4. Relance los pasos 2-3 para las otras blancos usando la información del URL baja siguiente:

   Blanco: Centro porta API de la petición de la nube de Cisco
   Base URL: hostname> del <cp de https://: <RequestCenter SSL port>/RequestCenter
   El puerto SSL de RequestCenter del valor por defecto es 8443

   Blanco: Servicio web del Orchestrator del proceso de Cisco
   Base URL: hostname> del Orchestrator del <process de https://: Orchestrator SSL port>/WS/del <process
   El puerto SSL del Orchestrator del proceso predeterminado es 61526
5. El servidor de portal de los servicios de Cisco es un tipo diferente de blanco. Para configurar este clic doble de la blanco en él.
6. Haga clic en el cambio de la lengueta de la conexión el puerto del link del servicio al puerto

de ServiceLink SSL (el valor por defecto es 6443), cambie el puerto del centro de la petición al puerto de RequestCenter SSL (el valor por defecto es 8443). También seleccione “el portal del servicio del acceso vía el Secure Socket Layer (SSL)” y también “ignore el error del certificado del Secure Socket Layer (SSL)”.
7. Haga Click en OK para salvar los cambios. Observe que esta blanco verificará la conexión SSL con el servidor del catálogo del servicio. El servidor del catálogo del servicio necesita ejecutar y hacer el SSL configurar.

Configure los agentes de RequestCenter para utilizar el SSL

Ahora que configuran al Orchestrator de proceso los agentes de RequestCenter necesitan ser configurados para utilizar el SSL.

1. Registro en la consola Web del catálogo del servicio como el Usuario administrador.
2. De la desconexión selecta “mi espacio de trabajo” y va al “asistente de configuración”. Si no está en “mi espacio de trabajo” entonces hace clic en “+” y agreguelo.
3. Haga clic el siguiente paso para ir al paso 1 y seleccionar “fijó la Configuración del agente HTTP”
4. Para “el servicio de red de proceso del Orchestrator URL” ingrese

   hostname> del Orchestrator del <process de https://: Port> del Orchestrator SSL del <process

   donde está el hostname> del Orchestrator del <process el nombre de host o la dirección IP del port> de proceso del servidor del Orchestrator y del Orchestrator SSL del <process es el puerto SSL de Orchestrator de proceso. El puerto predeterminado es 61526.
5. Para el nombre de usuario de proceso del Orchestrator, la contraseña, y el dominio ingresan en un nombre de usuario, una contraseña, y un dominio para el usuario que conectará con el servidor de proceso del Orchestrator.
6. Para “el link URL del Servicio de catálogo del servicio” ingrese

   hostname> del <cp de https://: <ServiceLink SSL port>/IntegrationServer

   donde está el hostname> del <cp el nombre de host o la dirección IP del port> del servidor y del <ServiceLink SSL del catálogo del servicio es el puerto SSL de ServiceLink. El puerto predeterminado es 6443.
7. El tecleo somete la orden.
8. Cierre la ventana de respuesta de la orden del someter.
9. Después de que la orden haya completado, haga clic en el “comienzo el resto de los agentes”. Si los agentes entonces se comienzan ya necesitan ser parados y ser comenzados otra vez para que la nueva configuración tome el efecto.
10. Seleccione todos los agentes en la página 1 y haga clic la “parada seleccionada”
11. Seleccione sí en la ventana de confirmación.
12. Relance los pasos 10-11 para todas las otras páginas.
13. Vuelva paginar 1, seleccionar todos los agentes y tecleo “comienzo seleccionado”
14. Seleccione sí en la ventana de confirmación.
15. Relance los pasos 13-14 para todas las otras páginas.

Configurando RequestCenter y ServiceLink para utilizar el SSL para comunicar (opcional)

¿El último paso es opcional? configurar RequestCenter y ServiceLink para utilizar el SSL para comunicar.

1. En el servidor del catálogo del servicio, abra su editor de archivos preferido.
2. Abra el archivo <JBOSS_RC_HOME> \ RequestCenterServer \ implementaciones \ RequestCenter.war \ Red-INF-clases \ config \ newscale.properties.
3. Busque para el <cp hostname>:6080 isee.base.url= http:// donde está el nombre de host el hostname> del <cp del servidor del catálogo del servicio.
4. Cambie la línea para ser el <cp hostname>:6443 isee.base.url= https://. El puerto 6443 es el puerto predeterminado para ServiceLink SSL. Si usted está utilizando un diverso puerto después ingreselo en vez de 6443.
5. Salve el archivo newscale.properties.
6. Recomience RequestCenter.