La portée de ce document est une revue du projet simple sur configurer le SSL sur le Cisco Intelligent Automation en nuage. Cette configuration utilisera les Certificats auto-signés mais peut être utilisée avec la tierce partie ou les certificats racine de confiance. Ce n'est pas un remplacement pour aucune documentation SSL dans le dossier de documentation IAC.

- Configurer le SSL sur le serveur de catalogue de service
- Configurer le SSL sur le serveur de processus d'orchestrator
- Configurant le catalogue de processus d'orchestrator et de service pour utiliser le SSL les uns avec les autres
- Configurant RequestCenter et ServiceLink pour employer le SSL pour communiquer (facultatif)

Le serveur de catalogue de service se compose de deux composants qui seront configurés pour le SSL : RequestCenter et ServiceLink. Cette configuration a été faite sur une configuration de JBoss de deux-serveur mais devrait travailler sur une configuration de JBoss d'un-serveur aussi bien. Cette configuration travaillera sur un serveur de catalogue de service de Windows ou Linux. Les étapes afficheront la configuration sur un serveur de catalogue de service windows mais peuvent être utilisées sur un serveur de catalogue de service de Linux. Dans les étapes au-dessous du **<JBOSS_RC_HOME>** variable se rapporte au répertoire home de JBoss pour RequestCenter, **<JBOSS_SL_HOME>** se rapporte au répertoire home de JBoss pour ServiceLink, et **<JAVA_HOME>** se rapporte au répertoire home de Javas.
Cette section contient les thèmes suivants :

- Configurer le SSL sur RequestCenter
- Configurer le SSL sur ServiceLink

Configurer le SSL sur RequestCenter

Cette section contient les thèmes suivants :

- Créez le certificat
- Certificat d'exportation
- Certificat d'importation à la mémoire de confiance de JBoss
- Certificat d'importation dans la mémoire de confiance de Javas
- Éditez le fichier de configuration standalone-full.xml

Créez le certificat

La première chose à faire est de créer un certificat auto-signé.

1. Ouvrez une invite de commande.
2. Changez les répertoires à **<JBOSS_RC_HOME> \ à RequestCenterServer \ à configuration**.
3. Créez un certificat auto-signé en exécutant la commande **<JAVA_HOME> \ jre \ coffre \ keytool - genkey - alias alias> de <requestcenter - le keyalg RSA - password> de <keypass de keypass - password> de <storepass de storepass - le keystore keystore.jks**

   Aux fins de la configuration le pseudonyme utilisé est **RequestCenter** et les keypass et le mot

de passe de storepass est le **changeit de** mot de passe par défaut.

REMARQUE: Vous serez incité à écrire des informations sur ce certificat. La première demande est **ce qui est votre premier et nom de famille** (également appelés la NC). Ceci doit être le nom de la machine ou le **localhost d'**hôte. Le reste des informations peut être celui que vous vouliez mettre dedans.

Certificat d'exportation

La prochaine chose à faire est d'exporter le certificat à un fichier.

1. Ouvrez une invite de commande.
2. Changez les répertoires à **<JBOSS_RC_HOME> \ à RequestCenterServer \ à configuration**.
3. Exportez le certificat à un fichier en exécutant la commande **<JAVA_HOME> \ jre \ coffre \ keytool - exportation - alias alias> de <requestcenter - password> de <storepass de storepass - classent le nom du fichier de certificat de <requestcenter > - le keystore keystore.jks**

   Aux fins de la configuration le nom du fichier utilisé est **RequestCenter.cer**.

Certificat d'importation à la mémoire de confiance de JBoss

La prochaine chose à faire est d'importer le certificat dans la mémoire de confiance de JBoss.

1. Ouvrez une invite de commande.
2. Changez les répertoires à **<JBOSS_RC_HOME> \ à RequestCenterServer \ à configuration**.
3. Importez le certificat dans la mémoire de confiance de JBoss en exécutant la commande **<JAVA_HOME> \ jre \ coffre \ keytool - importation - v - des trustcacerts - alias alias> de <requestcenter - classez le nom du fichier de certificat de <requestcenter > - le keystore cacerts.jks - password> de <keypass de keypass - password> de <storepass de storepass.**

Certificat d'importation dans la mémoire de confiance de Javas

La prochaine chose à faire est d'importer le certificat dans la mémoire de confiance de Javas.

1. Ouvrez une invite de commande.
2. Changez les répertoires à **<JAVA_HOME> \ à jre \ à bibliothèque \ à Sécurité**.
3. Copiez le fichier du certificat de RequestCenter de <JBOSS_RC_HOME> \ de RequestCenterServer \ de configuration dans ce répertoire.
4. Importez le certificat dans la mémoire de confiance de Javas en exécutant la commande **<JAVA_HOME> \ jre \ coffre \ keytool - importation - v - des trustcacerts - alias alias> de <requestcenter - classez le nom du fichier de certificat de <requestcenter > - des cacerts de keystore - password> de <keypass de keypass - password> de <storepass de storepass**.

Éditez le fichier de configuration standalone-full.xml

La prochaine chose à faire est d'éditer le fichier de configuration standalone-full.xml.

1. Ouvrez le fichier **<JBOSS_RC_HOME> \ RequestCenterServer \ configuration \ standalone-**

full.xml avec un éditeur de texte compétent.
2. Recherchez le name= socket-binding= le " HTTP »/> de " de <connector HTTP » de scheme= du " HTTP » protocol="HTTP/1.1" et ajoutez les lignes suivantes après lui :

   secure= " de " https de socket-binding= » de " https » de scheme= de " https » de name= du <connector protocol="HTTP/1.1" vrai " >
   certificate-key-file= " de " changeit de password= » de " alias> » de <requestcenter de key-alias= de <ssl <JBOSS_RC_HOME> \ RequestCenterServer \ configuration \ keystore.jks »/> </connector>

   REMARQUE: Alias> de <requestcenter de modification au RequestCenter alias que vous utilisez et <JBOSS_RC_HOME> au répertoire home de JBoss pour RequestCenter.
3. Sauvegardez le fichier standalone-full.xml.
4. Reprise RequestCenter.

Configurer le SSL sur ServiceLink

Pour configurer le SSL sur ServiceLink, répétez les étapes dans le SSL configurant sur la section de RequestCenter du document, vous veillant utilisez le répertoire <JBOSS_SL_HOME> et l'alias> de <servicelink.

Configurer le SSL sur le serveur de processus d'orchestrator

Le serveur de processus d'orchestrator est des Windows Server qui utilisent IIS. Cette section contient les thèmes suivants :

- Créez le certificat
- Certificat d'exportation
- Certificat de grippage pour traiter le port SSL d'orchestrator

Créez le certificat

La première chose à faire est de créer un certificat auto-signé.

1. Ouvrez le gestionnaire IIS.
2. Du côté gauche de la fenêtre, sélectionnez le serveur de processus d'orchestrator.
3. Du côté droit de la fenêtre, double clic sur des Certificats de serveur.
4. Du côté droit le côté d'extrême droite des fenêtres de Certificats de serveur, cliquez sur en fonction le certificat Auto-signé Create.
5. Écrivez un nom amical pour le certificat et cliquez sur OK.

Certificat d'exportation

1. Après que le certificat soit créé, cliquez avec le bouton droit là-dessus et sélectionnez la vue.

2. Cliquez sur en fonction l'onglet de détails et cliquez sur en fonction la copie pour classer
3. Sur l'assistant d'exportation de certificat cliquez sur Next.
4. Choisi **« non, n'exportent pas la clé privée »** et cliquent sur Next.
5. **X.509 encodés par Base-64** choisis **(.CER)** et cliquent sur Next.
6. Écrivez un nom du fichier et cliquez sur Next.
7. Cliquez sur Finish pour sauvegarder le fichier du certificat.

Certificat de grippage pour traiter le port SSL d'orchestrator

1. Ouvrez le fichier du certificat, cliquez sur en fonction l'onglet de détails, et faites descendre l'écran à Thumbprint dans la section de champ de la copie de tableau de détails la valeur hexadécimale pour Thumbprint - c'est la valeur de hachage de certificat.
2. Ouvrez une invite de commande.
3. HTTP de netsh exécutez commande « ajoutent le certhash=<thumbprint> appid={1776a671-8e9c-45b0-8304-dec6f472131f}" du sslcert ipport=0.0.0.0:61526

   L'ipport=0.0.0.0:61526 est l'adresse IP et port SSL pour l'orchestrator de processus. Il devrait être 0.0.0.0:61526.

   Le certhash est la valeur de Thumbprint que vous avez copiée dans l'étape 1.

   *NOTE : Vous devez enlever les espaces en valeur de Thumbprint. L'appid est toujours {1776a671-8e9c-45b0-8304-dec6f472131f}.

Configurant le catalogue de processus d'orchestrator et de service pour utiliser le SSL les uns avec les autres

Maintenant que le SSL est configuré sur le catalogue de service et l'orchestrator de processus, ces serveurs doivent être configurés pour communiquer les uns avec les autres utilisant le SSL. Pour faire que les serveurs doivent se faire confiance. Cela est fait en ajoutant les fichiers du certificat de serveur dans la mémoire de confiance. Cette section contient les thèmes suivants :

- Ajouter les Certificats de catalogue de service à la mémoire de processus de confiance d'orchestrator
- Ajouter les Certificats d'orchestrator de processus à la mémoire de confiance de catalogue de service
- Configurer le serveur de processus d'orchestrator pour utiliser le SSL
- Configurez les agents de RequestCenter pour utiliser le SSL

Ajouter les Certificats de catalogue de service à la mémoire de processus de confiance d'orchestrator

Le serveur de processus d'orchestrator doit avoir les Certificats du serveur de catalogue de

service (les Certificats de RequestCenter et de ServiceLink) installé dans sa mémoire de confiance.

1. Copiez les fichiers du certificat de RequestCenter et de ServiceLink sur le serveur de processus d'orchestrator.
2. Le clic droit sur le fichier du certificat de RequestCenter et sélectionnent « installent le certificat ».
3. Sur la fenêtre d'assistant d'importation de certificat cliquez sur Next.
4. Le « endroit choisi tous les Certificats dans la mémoire suivante » et le clic parcourent.
5. Sélectionnez les « Autorités de certification racine approuvée » et cliquez sur OK.
6. Cliquez sur Next
7. Cliquez sur Finish pour se terminer l'installation de certificat.
8. Un message d'erreur peut s'afficher en vue de le certificat le réclamant est de « localhost ». Cette erreur est correcte. Cliquez sur oui pour installer le certificat.
9. Sur la dernière fenêtre, cliquez sur OK pour compléter le processus d'installation.
10. Répétez les étapes 2-9 pour installer le certificat de ServiceLink.

Ajouter les Certificats d'orchestrator de processus à la mémoire de confiance de catalogue de service

Le serveur de catalogue de service doit avoir le certificat du serveur de processus d'orchestrator installé dans sa mémoire de confiance.

1. Ouvrez une invite de commande.
2. Changez les répertoires à <JAVA_HOME> \ à jre \ à bibliothèque \ à Sécurité.
3. Copiez le fichier du certificat de processus d'orchestrator sur le serveur de catalogue de service dans le répertoire <JAVA_HOME> \ jre \ bibliothèque \ Sécurité.
4. Importez le certificat dans la mémoire de confiance de Javas en exécutant la commande **<JAVA_HOME> \ jre \ coffre \ keytool - importation - v - des trustcacerts - alias alias> d'orchestrator de <Process - nom du fichier de certificat d'orchestrator de <Process de fichier > - des cacerts de keystore - password> de <keypass de keypass - password> de <storepass de storepass**.
5. Reprise RequestCenter et ServiceLink.

Configurer le serveur de processus d'orchestrator pour utiliser le SSL

Le serveur de processus d'orchestrator doit être configuré pour utiliser le SSL. Les propriétés de serveur et les diverses cibles doivent être configurées pour utiliser le SSL. Cette section contient les thèmes suivants :

- Changez les propriétés de serveur (les propriétés d'environnement)
- Configurez les cibles

Changez les propriétés de serveur (les propriétés d'environnement)

1. Ouvrez-vous et connectez-vous dans la console de processus d'orchestrator.

2. Du menu File, serveur Properties choisi (environnement Properties dans IAC 4.0).
3. Sélectionnez l'onglet de service Web
4. Désélectionnez « le service Web non-sécurisé d'enable (HTTP) » et sélectionnez « le service Web sécurisé d'enable (HTTPS) ». Vous pouvez voir le message suivant :

   L'activation des services Web de processus d'orchestrator de Cisco sur un port sécurisé (HTTPS) exige la configuration manuelle supplémentaire. Veuillez se référer à la documentation pour des instructions.

   Cliquez sur OK sur ce message.
5. Vous pouvez sélectionner un port HTTPS mais le par défaut de 61526 devrait être correct.
6. Le clic « régénèrent le service Web » et puis cliquent sur en fonction CORRECT.

Configurez les cibles

Les cibles « Cisco opacifient l'intégration portaile API », « Cisco opacifient le centre portail API de demande », « le service Web de processus d'orchestrator de Cisco », et « le serveur portail de Cisco Service » tout le besoin d'être configuré pour utiliser HTTPS et le port SSL.

1. Sur la console de processus d'orchestrator, sur en bas à gauche la partie des définitions choisies de fenêtre, sur en haut à gauche la partie des cibles choisies de fenêtre, et du côté droit du double clic de fenêtre sur « Cisco opacifient la cible de l'intégration API portail ».
2. Cliquez sur en fonction la modification d'onglet Connection l'URL de base à :

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

   là où le hostname> de <cp est l'adresse Internet ou l'adresse IP du port> de serveur de catalogue de service et SSL de <ServiceLink est le port SSL de ServiceLink. Le port par défaut est 6443.
3. Cliquez sur OK pour sauvegarder des modifications.
4. Répétez les étapes 2 ou 3 pour les autres cibles utilisant les informations suivantes URL de base :

   Cible : Cisco opacifient le centre portail API de demande
   URL de base : hostname> de <cp de https:// : SSL port>/RequestCenter de <RequestCenter
   Le port SSL de RequestCenter de par défaut est 8443

   Cible : Service Web d'orchestrator de processus de Cisco
   URL de base : hostname> d'orchestrator de <Process de https:// : SSL port>/WS/d'orchestrator de <Process
   Le port de processus par défaut SSL d'orchestrator est 61526
5. Le serveur portail de Cisco Service est un type différent de cible. Pour configurer ce double clic de cible là-dessus.
6. Cliquez sur en fonction la modification d'onglet Connection le port de lien de service au port SSL de ServiceLink (le par défaut est 6443), changez le port de centre de demande au port SSL de RequestCenter (le par défaut est 8443). Le « portail en outre choisi de service d'accès par l'intermédiaire du Protocole SSL (Secure Socket Layer) » et également

« ignorent l'erreur de certificat de Protocole SSL (Secure Socket Layer) ».
7. Cliquez sur OK pour sauvegarder des modifications. Notez que cette cible vérifiera la connexion SSL avec le serveur de catalogue de service. Le serveur de catalogue de service doit exécuter et faire configurer le SSL.

Configurez les agents de RequestCenter pour utiliser le SSL

Maintenant que l'orchestrator de processus est configuré les agents de RequestCenter doivent être configurés pour utiliser le SSL.

1. Connectez-vous dans la console Web de catalogue de service en tant qu'utilisateur d'admin.
2. Du menu déroulant choisi « mon espace de travail » et vont au « assistant de configuration ». S'il n'est pas sur « mon espace de travail » cliquent sur alors en fonction « + » et ajoutez-le.
3. Cliquez sur Next l'étape pour passer à l'étape 1 et sélectionner « a placé la configuration d'agent de HTTP »
4. Pour « l'URL de processus de service Web d'orchestrator » entrez

   hostname> d'orchestrator de <Process de https:// : Port> SSL d'orchestrator de <Process

   là où le hostname> d'orchestrator de <Process est l'adresse Internet ou l'adresse IP du port> de processus SSL de serveur d'orchestrator et d'orchestrator de <Process est le port SSL de l'orchestrator de processus. Le port par défaut est 61526.
5. Pour le nom d'utilisateur de processus d'orchestrator, le mot de passe, et le domaine entrent dans un nom d'utilisateur, un mot de passe, et un domaine pour l'utilisateur qui se connectera au serveur de processus d'orchestrator.
6. Pour « l'URL de lien de service de catalogue de service » entrez

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

   là où le hostname> de <cp est l'adresse Internet ou l'adresse IP du port> de serveur de catalogue de service et SSL de <ServiceLink est le port SSL de ServiceLink. Le port par défaut est 6443.
7. Cliquez sur Submit la commande.
8. Fermez la fenêtre de réponse de commande de soumission.
9. Après que la commande se soit terminée, cliquez sur en fonction le « début tous autres agents ». Si les agents sont déjà commencés alors ils doivent être arrêtés et commencés de nouveau pour que la nouvelle configuration la prenne effet.
10. Sélectionnez tous les agents à la page 1 et cliquez sur le « arrêt sélectionné »
11. Sélectionnez oui sur la fenêtre de confirmation.
12. Répétez les étapes 10-11 pour toutes les autres pages.
13. Retournez pour paginer 1, pour sélectionner tous les agents et clic « début sélectionné »
14. Sélectionnez oui sur la fenêtre de confirmation.
15. Répétez les étapes 13-14 pour toutes les autres pages.

Configurant RequestCenter et ServiceLink pour

employer le SSL pour communiquer (facultatif)

La dernière étape est facultative ? configurer RequestCenter et ServiceLink pour employer le SSL pour communiquer.

1. Sur le serveur de catalogue de service, ouvrez votre éditeur préféré de fichier.
2. Ouvrez le fichier <JBOSS_RC_HOME> \ RequestCenterServer \ déploiements \ RequestCenter.war \ Web-FNI-classes \ config \ newscale.properties.
3. Recherchez le <cp hostname>:6080 isee.base.url= http:// où le hostname> de <cp est l'adresse Internet du serveur de catalogue de service.
4. Changez la ligne pour être le <cp hostname>:6443 isee.base.url= https://. Le port 6443 est le port par défaut pour le SSL de ServiceLink. Si vous utilisez un port différent alors entrez-dansle au lieu de 6443.
5. Sauvegardez le fichier newscale.properties.
6. Reprise RequestCenter.