Область этого документа является простой пошаговой демонстрацией при настройке SSL на Cisco Intelligent Automation for Cloud. Эта конфигурация будет использовать подписанные сертификаты, но может использоваться с Независимым поставщиком или Сертификатами доверенного корня. Это не замена ни для какой документации SSL в портфеле документации IAC.

- SSL Настройки на сервере Каталога услуг
- SSL Настройки на сервере Дирижера Процесса
- Дирижер Процесса Настройки и Каталог услуг для использования SSL друг с другом
- Настройка RequestCenter и ServiceLink для использования SSL для передачи (дополнительный)

Сервер Каталога услуг состоит из двух компонентов, которые будут настроены для SSL: RequestCenter и ServiceLink. Эта конфигурация была реализована на конфигурации JBoss с двумя серверами, но должна работать на конфигурацию JBoss с одним сервером также. Эта конфигурация будет работать на Windows или сервер Каталога услуг Linux. Шаги покажут конфигурацию на сервере Каталога службы Windows, но могут использоваться на сервере Каталога услуг Linux. В шагах ниже переменной **<JBOSS_RC_HOME>** ссылается на главный каталог JBoss для RequestCenter, **<JBOSS_SL_HOME>** ссылается на главный каталог JBoss для ServiceLink, и **<JAVA_HOME>** ссылается на главный каталог Java.
В этом разделе рассматриваются следующие темы:

- SSL Настройки на RequestCenter
- SSL Настройки на ServiceLink

SSL Настройки на RequestCenter

В этом разделе рассматриваются следующие темы:

- Создайте сертификат
- Сертификат экспорта
- Сертификат импорта к базе доверенных сертификатов JBoss
- Сертификат импорта в базе доверенных сертификатов Java
- Отредактируйте автономный-full.xml файл конфигурации

Создайте сертификат

Первое, что нужно сделать состоит в том, чтобы создать подписанный сертификат.

1. Откройте командную строку.
2. Каталоги изменения к **<JBOSS_RC_HOME> \RequestCenterServer\configuration**.
3. Создайте подписанный сертификат путем выполнения **команды <JAVA_HOME> \jre\bin\keytool - genkey - псевдоним <requestcenter псевдоним>-keyalg RSA-keypass <keypass пароль>-storepass <storepass пароль>-keystore keystore.jks**

   В целях конфигурации используемым псевдонимом является **RequestCenter** и keypass, и storepass пароль является паролем по умолчанию **changeit**.

Примечание: Вам предложат ввести информацию об этом сертификате. Первое приглашение - **то, Что является вашим именем и фамилиенем** (также названный CN). Это должно быть именем хоста машины или **локального узла**. Остаток информации может быть тем, что вы хотите вставить.

Сертификат экспорта

Следующая вещь сделать состоит в том, чтобы экспортировать сертификат в файл.

1. Откройте командную строку.
2. Каталоги изменения к **<JBOSS_RC_HOME> \RequestCenterServer\configuration**.
3. Экспортируйте сертификат в файл путем выполнения **команды <JAVA_HOME> \jre\bin\keytool - экспорта - псевдонима <requestcenter псевдоним>-storepass <storepass пароль> - файл <requestcenter name> файла сертификата-keystore keystore.jks**

   В целях конфигурации используемое имя файла является **RequestCenter.cer**.

Сертификат импорта к базе доверенных сертификатов JBoss

Следующая вещь сделать состоит в том, чтобы импортировать сертификат в базу доверенных сертификатов JBoss.

1. Откройте командную строку.
2. Каталоги изменения к **<JBOSS_RC_HOME> \RequestCenterServer\configuration**.
3. Импортируйте сертификат в базу доверенных сертификатов JBoss путем выполнения **команды <JAVA_HOME> \jre\bin\keytool - импортируют-v-trustcacerts - псевдоним <requestcenter псевдоним> - файл <requestcenter name> файла сертификата-keystore cacerts.jks-keypass <keypass пароль>-storepass <storepass пароль>**.

Сертификат импорта в базе доверенных сертификатов Java

Следующая вещь сделать состоит в том, чтобы импортировать сертификат в Базу доверенных сертификатов Java.

1. Откройте командную строку.
2. Каталоги изменения к **<JAVA_HOME> \jre\lib\security**.
3. Скопируйте файл сертификата RequestCenter с <JBOSS_RC_HOME> \RequestCenterServer\configuration в этот каталог.
4. Импортируйте сертификат в базу доверенных сертификатов Java путем выполнения **команды <JAVA_HOME> \jre\bin\keytool - импортируют-v-trustcacerts - псевдоним <requestcenter псевдоним> - файл <requestcenter name> файла сертификата-keystore cacerts-keypass <keypass пароль>-storepass <storepass пароль>**.

Отредактируйте автономный-full.xml файл конфигурации

Следующая вещь сделать состоит в том, чтобы отредактировать автономный-full.xml файл конфигурации.

1. Откройте **файл <JBOSS_RC_HOME> \RequestCenterServer\configuration\standalone-full.xml** с соответствующим текстовым редактором.
2. Поиск **<название разъёма = протокол "http" = схема "HTTP/1.1" = привязка сокета "http" = "http"/>** и добавляет следующие линии после него:

   <протокол разъёма = название "HTTP/1.1" = схема "https" = привязка сокета "https" = "https" защищают = "истинный">
   <ssl ключевой псевдоним = "<requestcenter псевдоним>" пароль = "changeit"
   контрольный файл сертификата = "<JBOSS_RC_HOME>
   \RequestCenterServer\configuration\keystore.jks"/>
   </разъём>

   Примечание: Изменение **<requestcenter псевдоним>** к псевдониму RequestCenter вы используете и **<JBOSS_RC_HOME>** для главного каталога JBoss для RequestCenter.
3. Сохраните **автономный-full.xml** файл.
4. Перезапуск RequestCenter.

SSL Настройки на ServiceLink

Для настройки SSL на ServiceLink повторите шаги в SSL Настройки на разделе RequestCenter документа, удостоверившись, что вы используете каталог **<JBOSS_SL_HOME>** и <servicelink псевдоним>.

SSL Настройки на сервере Дирижера Процесса

Сервером Дирижера Процесса является Windows Server, который использует IIS. В этом разделе рассматриваются следующие темы:

- Создайте сертификат
- Сертификат экспорта
- Свяжите сертификат Обрабатывать порт SSL Дирижера

Создайте сертификат

Первое, что нужно сделать состоит в том, чтобы создать подписанный сертификат.

1. Открытый диспетчер IIS.
2. На левой части окна выберите сервер Дирижера Процесса.
3. На правой части окна дважды нажмите на Server Certificates.
4. На дальней правой стороне окон Server Certificates щелкните по Create Self-Signed Certificate.
5. Введите дружественное имя для сертификата и нажмите OK.

Сертификат экспорта

1. После того, как сертификат создан, щелкните правой кнопкой мыши на нем и выберите View.
2. Щелкните по вкладке Details и щелкните по Copy to File
3. На Сертификате Мастер Экспорта нажимают **Next**.
4. Выберите **"No, do not export private key"** и нажмите **Next**.
5. Выберите **закодированный x.509 Base-64 (.CER)** и нажмите **Next**.
6. Введите имя файла и нажмите **Next**.
7. Нажмите **Finish** для сохранения файла сертификата.

Свяжите сертификат Обрабатывать порт SSL Дирижера

1. Откройте файл сертификата, щелкните по вкладке Details и прокрутите вниз к Следу большого пальца в Полевом разделе вкладки Details. Скопируйте Шестнадцатеричное значение для Следа большого пальца - это - значение хеш-функции сертификата.
2. Откройте командную строку.
3. Выполните команду "netsh, http добавляют sslcert ipport=0.0.0.0:61526 certhash = <след большого пальца> appid = {1776a671-8e9c-45b0-8304-dec6f472131f}"

   ipport=0.0.0.0:61526 является IP-адрес и порт SSL для Дирижера Процесса. Это должно быть 0.0.0.0:61526.

   certhash является значением Следа большого пальца, которое вы скопировали в Шаге 1.

   Примечание: Необходимо удалить пробелы в значении Следа большого пальца. appid всегда {1776a671-8e9c-45b0-8304-dec6f472131f}.

Дирижер Процесса Настройки и Каталог услуг для использования SSL друг с другом

Теперь, когда SSL настроен на Дирижере Каталога услуг и Процесса, эти серверы должны быть настроены для передачи друг с другом использующим SSL. Чтобы сделать это, серверы должны доверять друг другу. Это сделано путем добавления файлов серверного сертификата в Базу доверенных сертификатов. В этом разделе рассматриваются следующие темы:

- Добавление сертификатов Каталога услуг к базе доверенных сертификатов Дирижера Процесса
- Добавление сертификатов Дирижера Процесса к базе доверенных сертификатов Каталога услуг
- Настройка сервер Дирижера Процесса для использования SSL
- Настройте Агентов RequestCenter для использования SSL

Добавление сертификатов Каталога услуг к базе доверенных сертификатов Дирижера Процесса

Сервер Дирижера Процесса должен иметь сертификаты сервера Каталога услуг (и сертификаты RequestCenter и ServiceLink) установленный в его Базе доверенных сертификатов.

1. Скопируйте файлы сертификата RequestCenter и ServiceLink на сервер Дирижера Процесса.
2. Щелкните правой кнопкой мыши на файле сертификата RequestCenter и выберите "Install Certificate".
3. На Сертификате Окно мастера Импорта нажимают Next.
4. Выберите "Place all certificates in the following store" и нажмите Browse.
5. Выберите "Trusted Root Certification Authorities" и нажмите OK.
6. Нажмите кнопку Next
7. Нажмите Finish для завершения установки сертификатов.
8. Сообщение об ошибках может появиться в отношении сертификата, утверждая, что это от "локального узла". Эта ошибка хорошо. Нажмите Yes для установки сертификата.
9. На последнем окне нажмите OK для завершения процесса установки.
10. Повторите Шаги 2-9 для установки сертификата ServiceLink.

Добавление сертификатов Дирижера Процесса к базе доверенных сертификатов Каталога услуг

Сервер Каталога услуг должен иметь сертификат сервера Дирижера Процесса, установленного в его Базе доверенных сертификатов.

1. Откройте командную строку.
2. Каталоги изменения к <JAVA_HOME> \jre\lib\security.
3. Скопируйте файл сертификата Дирижера Процесса к серверу Каталога услуг в <JAVA_HOME> \jre\lib\security каталог.
4. Импортируйте сертификат в базу доверенных сертификатов Java путем выполнения **команды <JAVA_HOME> \jre\bin\keytool - импортируют-v-trustcacerts - псевдоним Дирижера <Process псевдонима> - name> файла сертификата Дирижера <Process файла-keystore cacerts-keypass <keypass пароль>-storepass <storepass пароль>**.
5. Перезапустите RequestCenter и ServiceLink.

Настройка сервер Дирижера Процесса для использования SSL

Сервер Дирижера Процесса должен быть настроен для использования SSL. Свойства сервера и различные цели должны быть настроены для использования SSL. В этом разделе рассматриваются следующие темы:

- Измените свойства сервера (свойства среды)
- Настройте цели

Измените свойства сервера (свойства среды)

1. Откройтесь и войдите в Консоль Дирижера Процесса.
2. От Меню Файл выберите свойства сервера (Свойства среды в IAC 4.0).
3. Выберите вкладку веб-сервиса
4. Отмена выбора "Включает незащищенный веб-сервис (HTTP)" и выбирает "Enable secure Web Service (HTTPS)". Можно видеть следующее сообщение:

   Включение веб-сервисов Дирижера Процесса Cisco на защищенном порте (HTTPS) требует дополнительной настройки вручную. См. документацию для инструкций.

   Нажмите OK на этом сообщении.
5. Можно выбрать порт HTTPS, но по умолчанию 61526 должен быть хорошо.
6. Нажмите "Refresh Web Service" и затем щелкните по OK.

Настройте цели

Цели "Облачный API Интеграции порталов Cisco", "Облачный API Центра Запроса Портала Cisco", "веб-сервис Дирижера Процесса Cisco", и "Портальный сервер сервиса Cisco" вся потребность, которая будет настроена для использования HTTPS и порта SSL.

1. На консоли Дирижера Процесса, на левой нижней части окна выбирают Definitions, на вершине, оставленной часть окна, выбирают Targets, и на правой части двойного нажатия окна на "Облачной цели" API Интеграции порталов Cisco.
2. Щелкните по изменению вкладки Connection Базовый URL к:

   https://<имя хоста cpa>: <порт ServiceLink SSL>/IntegrationServer/services

   где <имя хоста cpa> является именем хоста, или IP-адрес сервера Каталога услуг и <порта ServiceLink SSL> является портом SSL ServiceLink. Порт по умолчанию 6443.
3. Нажмите OK для сохранения изменений.
4. Повторите Шаги 2-3 для других целей с помощью следующей информации о Базовом URL:

   Цель: облачный API центра запроса портала Cisco
   Базовый URL: https://<имя хоста cpa>: <порт RequestCenter SSL>/RequestCenter
   Порт RequestCenter SSL по умолчанию 8443

   Цель: веб-сервис дирижера процесса Cisco
   Базовый URL: https://имя хоста Дирижера <Process>: порт SSL Дирижера <Process>/WS/
   Порт SSL Дирижера Процесса по умолчанию 61526
5. Портальный сервер сервиса Cisco является разным типом цели. Настраивать это целевое двойное нажатие на нем.
6. Щелкните по изменению вкладки Connection порт Канала обслуживания к порту ServiceLink SSL (по умолчанию 6443), измените порт Центра Запроса на порт RequestCenter SSL (по умолчанию 8443). Также выберите "Access Service Portal via Secure Socket Layer (SSL)", и также "Игнорируют ошибку сертификата Протокола SSL".
7. Нажмите OK для сохранения изменений. Обратите внимание на то, что эта цель

проверит подключение SSL с сервером Каталога услуг. Сервер Каталога услуг должен работать и настраивать SSL.

Настройте Агентов RequestCenter для использования SSL

Теперь, когда Дирижер Процесса настроен, Агенты RequestCenter должны быть настроены для использования SSL.

1. Войдите в Веб - консоль Каталога услуг как в пользователя Admin.
2. От выпадающего выбирают "My workspace" и переходят к "Мастеру настройки". Если это не находится на "Моей Рабочей области", тогда щелкают "+" и добавляют его.
3. Нажмите Next Step, чтобы перейти к Шагу 1 и выбрать "Set HTTP Agent Configuration"
4. Для "URL веб-сервиса Дирижера Процесса" входят

   https://имя хоста Дирижера <Process>: порт SSL Дирижера <Process>

   где имя хоста Дирижера <Process> является именем хоста или IP-адресом сервера Дирижера Процесса, и порт SSL Дирижера <Process> является портом SSL Дирижера Процесса. Порт по умолчанию 61526.
5. Для Имени пользователя Дирижера Процесса Пароль и Домен входят в имени пользователя, пароле и домене для пользователя, который соединится с сервером Дирижера Процесса.
6. Для "URL Канала обслуживания Каталога услуг" входят

   https://<имя хоста cpa>: <порт ServiceLink SSL>/IntegrationServer

   где <имя хоста cpa> является именем хоста, или IP-адрес сервера Каталога услуг и <порта ServiceLink SSL> является портом SSL ServiceLink. Порт по умолчанию 6443.
7. Нажмите Submit Order.
8. Закройте окно ответа Submit Order.
9. После того, как Заказ завершил, Щелкните по "Start all other agents". Если агенты уже запущены тогда, они должны быть остановлены и запущены снова для новой конфигурации для вступления в силу.
10. Выберите всех агентов на Странице 1 и нажмите "Stop Selected"
11. Выберите Yes на окне подтверждения.
12. Повторите Шаги 10-11 для всех других страниц.
13. Вернитесь к Странице 1, выберите всех агентов и нажмите "Start Selected"
14. Выберите Yes на окне подтверждения.
15. Повторите Шаги 13-14 для всех других страниц.

Настройка RequestCenter и ServiceLink для использования SSL для передачи (дополнительный)

Заключительный шаг является дополнительным? настройка RequestCenter и ServiceLink для использования SSL для передачи.

1. На сервере Каталога услуг откройте своего любимого редактора файлов.
2. Откройте файл <JBOSS_RC_HOME> \RequestCenterServer\deployments\RequestCenter.war\WEB-INF-classes\config\newscale.properties.
3. Поиск isee.base.url=http://<имя хоста cpa>:6080, где <имя хоста cpa> является именем хоста сервера Каталога услуг.
4. Измените линию, чтобы быть isee.base.url=https://<имя хоста cpa>:6443. Порт 6443 является портом по умолчанию для ServiceLink SSL. При использовании другой порт, тогда вводят его вместо 6443.
5. Сохраните newscale.properties файл.
6. Перезапуск RequestCenter.