Создание сертификатов сервисов агента

Для работы агента требуются сертификаты:

- **CM Agent CA** – корневой сертификат сервисов агента. Используется для выдачи сертификатов рабочим станциям пользователей, на которых будут устанавливаться Агенты.
- **CM Agent SSL** – сертификат проверки подлинности, подписан корневым сертификатом. Необходим для установления двухстороннего защищенного соединения между сервером и рабочей станцией с установленным Агентом. Сертификат выдается на имя рабочей станции, на которой развернут сервер Indeed CM.
- **Сертификат рабочей станции** – выдается автоматически при регистрации клиентского агента. Обращаясь к серверу, клиентский компьютер предоставляет свой сертификат, а сервер Indeed CM проверяет его подлинность. После проверки сервер добавляет клиентский компьютер в список доверенных и может передавать на него задачи.

Сертификаты сервисов агента создаются при помощи утилиты **Cm.Agent.Cert.Generator**, входящей в состав дистрибутива системы (располагается в IndeedCM. Server\Misc\AgentCertGenerator).

Параметры утилиты

Генерация корневого и SSL-сертификата:

/root - генерация корневого сертификата сервисов агента.
/rootKeySize - размер закрытого ключа корневого сертификата сервисов агента (не обязательный параметр, по умолчанию генерируется закрытый ключ размером 4096 бит, возможный диапазон от 512 до 8192 бит).
/sn <*DNS-имя сервера*> - генерация SSL-сертификата на указанное DNS-имя сервера.
/csn - генерация SSL-сертификата на имя сервера, на котором запущена утилита.
/sslKeySize - размер закрытого ключа SSL-сертификата (необязательный параметр, по умолчанию генерируется закрытый ключ размером 2048 бит, возможный диапазон от 512 до 4096 бит).
/pwd - пароль SSL-сертификата (необязательный параметр).
/installToStore - публикует выпущенные утилитой сертификаты в хранилища сертификатов сервера (необязательный параметр, используется только для ОС Windows):

- Сертификат **CM Agent CA** в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities).
- Сертификат **CM Agent SSL** в хранилище **Личных** сертификатов рабочей станции, на которой установлен сервер Indeed CM.

Генерация только SSL-сертификата, используя уже выпущенный корневой сертификат CM Agent CA:

/rootKey - путь до файла корневого сертификата сервисов агента.
/ssl - генерация SSL-сертификата сервисов агента.
/sn <*DNS-имя сервера*> - генерация SSL-сертификата на указанное DNS-имя сервера.
/csn - генерация SSL-сертификата на имя сервера, на котором запущена утилита.
/pwd - пароль SSL-сертификата (необязательный параметр).
/sslKeySize - размер закрытого ключа SSL-сертификата (необязательный параметр, по умолчанию генерируется закрытый ключ размером 2048 бит, возможный диапазон от 512 до 4096 бит).
/installToStore - публикует выпущенный утилитой SSL-сертификат в хранилище **Личных** сертификатов рабочей станции, на которой установлен сервер системы (необязательный параметр, используется только для ОС Windows).

Запуск утилиты генерации сертификатов сервисов агента на ОС семейства Windows:

1. Запустите в командной строке, запущенной от имени администратора, на сервере Indeed CM утилиту с параметрами и дождитесь завершения её работы:

Пример:
Cm.Agent.Cert.Generator.exe /root /csn /installToStore

Запуск утилиты генерации сертификатов сервисов агента на ОС семейства Linux:

1. На сервере Indeed CM откройте терминал, перейдите в директорию с утилитой и измените права на файл, добавив право на выполнение файла **Cm.Agent.Cert.Generator:**

```
sudo chmod +x Cm.Agent.Cert.Generator
```

2. Запустите утилиту с параметрами: **/root /csn** и дождитесь завершение ее работы:

Пример:
./Cm.Agent.Cert.Generator /root /csn

В каталоге с утилитой появятся файлы:

- **agent_root_ca.json** - корневой сертификат сервисов агента с закрытым ключом в формате JSON.
- **agent_root_ca.cer** - корневой сертификат сервисов агента.
- **agent_root_ca.key** - закрытый ключ корневого сертификата сервисов агента.
- **agent_ssl_cert.cer** - SSL-сертификат сайта сервисов агента.
- **agent_ssl_cert.key** - закрытый ключ SSL-сертификата сайта сервисов агента.
- **agent_ssl_cert.pfx** - SSL-сертификат сервисов агента с закрытым ключом в формате PFX.

Поместите сертификат **CM Agent CA (agent_root_ca.cer)** в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на сервере системы.

Если в вашем окружении используется несколько серверов Indeed CM с агентами, то для каждого сервера требуется выпустить SSL-сертификат сервисов агента, используя общий корневой сертификат CM Agent CA (корневой сертификат сервисов агента на всех серверах должен быть один и тот же). Для создания SSL-сертификата дополнительного сервера или обновления истекшего сертификата перенесите каталог с утилитой **Cm.Agent.Cert.Generator** и корневой сертификат сервисов агента с закрытым ключом в формате JSON **(agent_root_ca.json)** на сервер и выполните команду:

```
Cm.Agent.Cert.Generator.exe /rootKey <путь к файлу agent_root_ca.json> /ssl /sn <DNS-имя сервера IndeedCM> /installToStore
```

Пример запуска утилиты для создания дополнительного или обновление истекшего SSL-сертификата сервисов агента:

ОС Windows:
```
Cm.Agent.Cert.Generator.exe /rootKey "C:\AgentCertGenerator\agent_root_ca.json" /ssl /sn indeedcm2.demo.local /installToStore
```

ОС Linux:
```
./Cm.Agent.Cert.Generator /rootKey ./agent_root_ca.json /ssl /sn indeedcm2.demo.local
```

Настройка защищенного соединения с сайтом сервисов агента

Для операционных систем семейства Windows

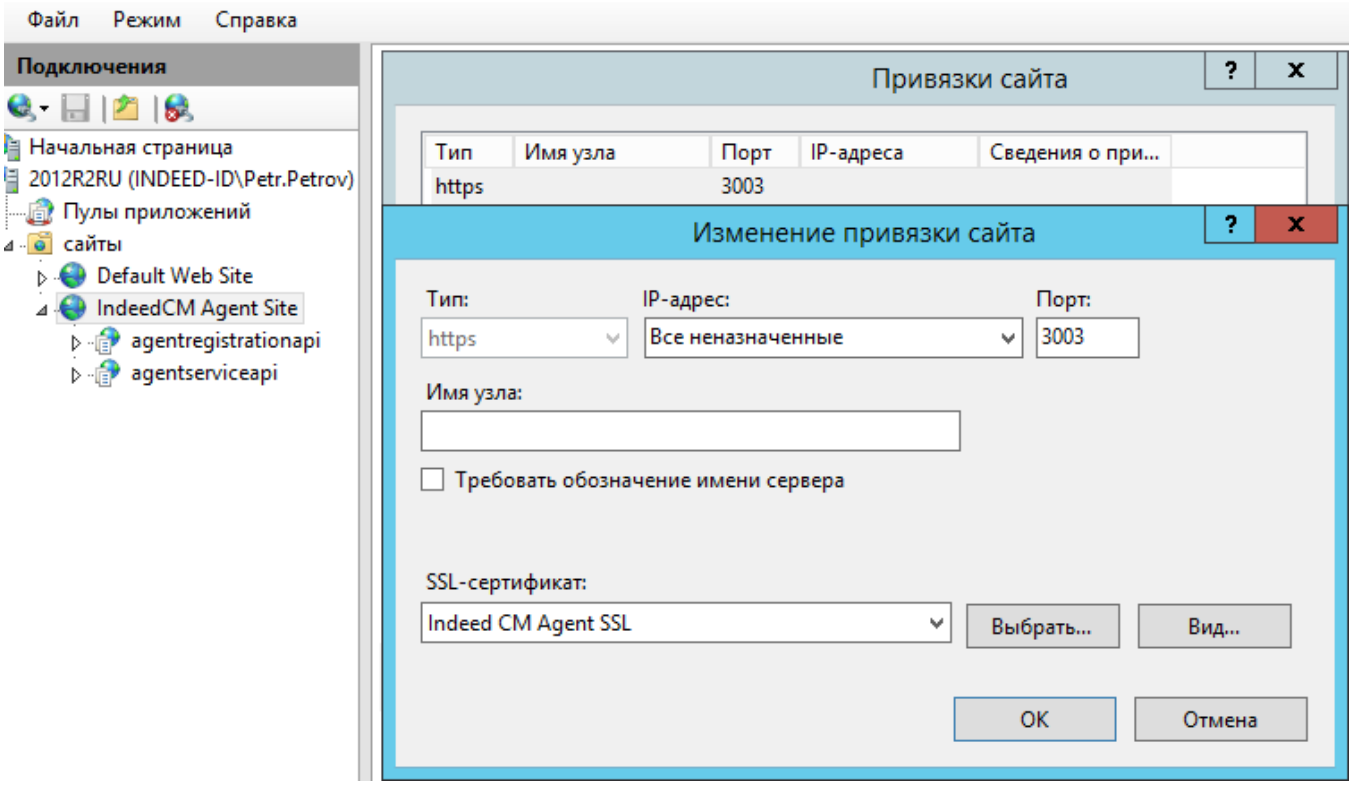
- Перейдите в **Диспетчер служб IIS** (Internet Information Services (IIS) Manager).
- Выберите сайт **IndeedCM Agent Site** и перейдите в раздел **Привязки...** (Bindings...).
- Выберите привязку по порту **3003**.
- Нажмите **Изменить...** (Edit...).
- Укажите в качестве **SSL-сертификата** сертификат **CM Agent SSL** или другой SSL /TLS-сертификат, выпущенный с любого доверенного УЦ в инфраструктуре на имя сервера системы и нажмите **OK**.

Порт **3003** устанавливается по умолчанию. Если вы используете другой порт, то создайте и настройте новую привязку для него. Убедитесь в том, что порт открыт для входящих подключений в брандмауэре.

В качестве SSL/TLS-сертификата допускается использование RSA-сертификата, выпущенного с любого доверенного УЦ на имя сервера Indeed CM.

- **Субъект** (Subject) сертификата должен содержать атрибут **Общее имя** (Common name) (FQDN сервера системы).
- **Дополнительное имя субъекта** (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера системы). Например: *indeedcm.demo.local* или соответствующую запись с подстановочными знаками, например: **. demo.local* (Wildcard certificate).
- **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).

Пример настройки привязки для сайта IndeedCM Agent Site.



Для операционных систем семейства Linux:

1. Скопируйте созданный утилитой SSL-сертификат сайта агентских сервисов и его приватный ключ в соответствующие хранилища на сервере Indeed CM, а также корневой сертификат Агента в хранилище доверенных корневых сертификатов:

   Пример

   ```
   sudo cp ./agent_ssl_cert.cer /etc/ssl/certs/
   sudo cp ./agent_ssl_cert.key /etc/ssl/private/
   sudo cp ./agent_root_ca.cer /usr/local/share/ca-certificates/
   ```

2. Запустите команду обновления хранилища доверенных корневых сертификатов:

   Пример

   ```
   sudo update-ca-certificates
   ```

3. Укажите пути до сертификата и закрытого ключа в конфигурационном файле используемого web-сервера в разделе описывающем сайт сервисов агента.

Пример конфигурационного файла web-сервера Nginx:

```
server {
    listen          3003 ssl;
    server_name     redos.demo.local;

    ssl_certificate    "/etc/ssl/certs/indeedcm.demo.local_ssl_cert.cer";
    ssl_certificate_key "/etc/ssl/private/indeedcm.demo.local_ssl_cert.key";
    ssl_verify_client   optional_no_ca;

    location /agentregistrationapi
       {  include /etc/nginx/conf.d/proxy.conf;
          proxy_pass http://localhost:5006/agentregistrationapi;  }
    location /agentserviceapi
     {  include /etc/nginx/conf.d/proxy.conf;
          proxy_pass http://localhost:5007/agentserviceapi;
          proxy_set_header x-ssl-client-cert $ssl_client_escaped_cert;  }
  }
}
```

⚠ Порт **3003** используется по умолчанию. Если вы используете другой порт, то создайте и настройте новую привязку для него. Убедитесь в том, что порт открыт для входящих подключений в брандмауэре.

В качестве SSL/TLS-сертификата допускается использование RSA-сертификата, выпущенного с любого доверенного УЦ на имя сервера Indeed CM.

- **Субъект** (Subject) сертификата должен содержать атрибут **Общее имя** (Common name) (FQDN сервера системы).
- **Дополнительное имя субъекта** (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера системы). Например: *indeedcm.demo.local* или соответствующую запись с подстановочными знаками, например: **. demo.local* (Wildcard certificate).
- **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).