Сервер NOMAD 2.10. Инструкция по настройке аутентификации по сертификатам

В документе описан порядок настройки аутентификации по сертификатам на сервере NOMAD и в мобильных приложениях DIRECTUM Solo и DIRECTUM Jazz.

Основные понятия

NOMAD (Native Offline Mobile Applications for DIRECTUM)

Нативные мобильные приложения для систем DIRECTUM и DirectumRX – DIRECTUM Jazz и DIRECTUM Solo. Предназначены для работы с документами, задачами и заданиями систем посредством мобильных устройств..

Сервер NOMAD

Набор серверных компонент, состоящий из веб-сервиса NOMAD и конфигуратора сервера NOMAD. Предназначен для выполнения функций, запрашиваемых клиентским приложением, предоставления доступа к данным и т.п.

Веб-сервис NOMAD

Серверное приложение, предоставляющее методы авторизации, доступа к данным системы DIRECTUM.

Конфигуратор сервера NOMAD

Приложение, предназначенное для проверки и изменения настроек, заданных при установке сервера NOMAD.

Общие сведения

Для аутентификации в приложениях DIRECTUM Solo для iOS и DIRECTUM Jazz для iOS поддерживаются только RSA-сертификаты.

Аутентификация по сертификату возможна при одновременном выполнении условий:

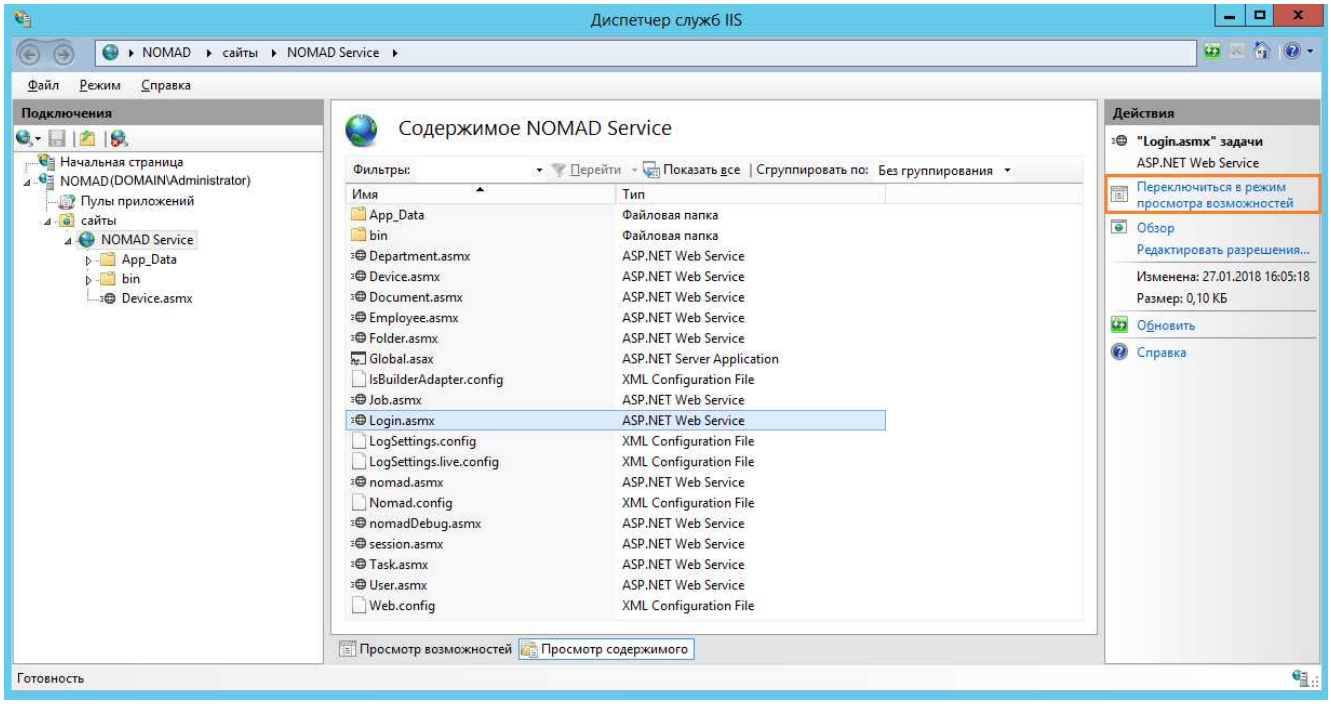
- веб-сервис NOMAD и клиентские приложения настроены на использование защищенного протокола HTTPS. Подробнее см. в документах «Сервер NOMAD. Инструкция по установке и удалению», «DIRECTUM Solo. Инструкция по установке и настройке», «DIRECTUM Jazz. Инструкция по установке и настройке», входят в комплект поставки;
- для входа в систему DIRECTUM используется Windows-аутентификация.

Возможность аутентификации в мобильном приложении по сертификату настраивается в конфигураторе сервера NOMAD на закладке «Настройки веб-сервиса». В группе полей «Тип аутентификации клиента» можно указать разрешенные способы входа в приложение: **По паролю**, **По сертификату**.

Настройка выполняется последовательно на сервере NOMAD и в клиентских приложениях DIRECTUM Solo и DIRECTUM Jazz.

Настройка на сервере NOMAD

1. Запустите **Диспетчер сервера** и добавьте службы ролей веб-сервера (IIS):
   - проверка подлинности с сопоставлением сертификата клиента;
   - проверка подлинности с сопоставлением сертификата клиента IIS.
2. Запустите оснастку «Диспетчер служб IIS».
3. Перейдите на уровень веб-сервера, выберите настройку **Проверка подлинности** и включите проверку подлинности клиента Active Directory с помощью сертификата.
4. В контекстном меню сайта выберите пункт **Переключиться в режим просмотра содержимого**.
5. Выберите login.asmx. В контекстном меню или на панели действий выберите пункт **Переключиться в режим просмотра возможностей**:



6. Выберите настройку **Параметры SSL** и установите переключатель **Принимать для сертификатов клиента**.
7. Настройте имена участников службы Service Principal Name (SPN).
8. Настройте доверие для делегирования служб Kerberos.

Настройка имен участников службы Service Principal Name (SPN)

1. Выполните команды:

   setspn -R NomadAdmin

   где **NomadAdmin** – учетная запись, от имени которой работает пул приложений.

   setspn -R NomadSBRTE

   где **NomadSBRTE** – учетная запись, от имени которой запускаются процессы SBRte.

2. Определите порт SQL-сервера:

   Запустите оснастку SQL Server Configuration Manager и последовательно выберите **Сетевая конфигурация SQL Server**, **Протоколы для <Имя экземпляра>**.

   В списке выберите протокол **TCP/IP**. Откроется окно свойств протокола TCP/IP.

   На вкладке «IP-адреса» проверьте наличие динамического порта TCP. По умолчанию SQL-сервер работает через порт 1433. В некоторых случаях, например, если на сервере используется несколько экземпляров SQL-сервера, номер порта может отличаться от стандартного.

3. Зарегистрируйте имя SPN для SQL-сервера:

   - если SQL-сервер работает от имени служебной учетной записи «Локальная система», то выполните команды:

     ```
     setspn -R SQLServerName
     setspn -S MSSQLSvc/SQLServerName.domain.local:SQLServerPort SQLServerName
     setspn -S MSSQLSvc/SQLServerName.domain.local SQLServerName
     ```

     где

     SQLServerName – имя SQL-сервера;

     domain.local – DNS-суффикс домена;

     SQLServerPort – порт SQL-сервера, определенный в п. 2;

   - если SQL-сервер работает от имени доменной учетной записи, то выполните команды:

     ```
     setspn -R SQLAdmin
     setspn -S MSSQLSvc/SQLServerName.domain.local:SQLServerPort SQLAdmin
     setspn -S MSSQLSvc/SQLServerName.domain.local SQLAdmin
     ```

     где

     SQLAdmin – учетная запись, от имени которой работает служба SQL-сервера;

     SQLServerName – имя SQL-сервера;

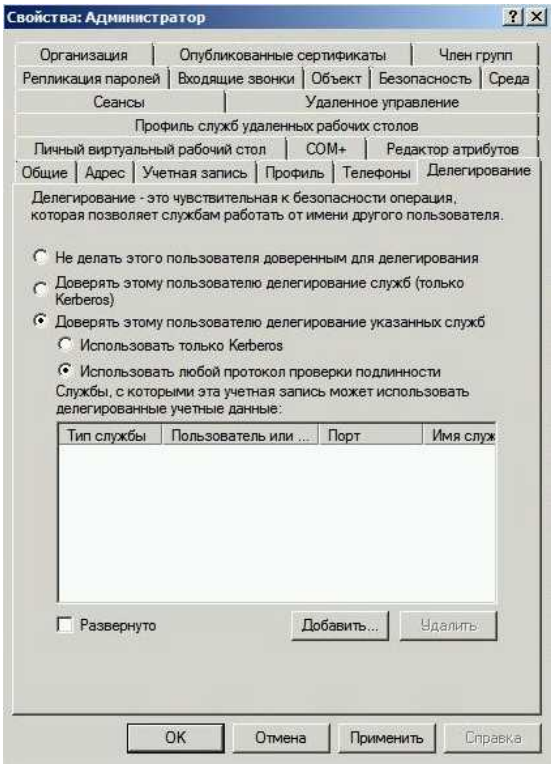
     domain.local – DNS-суффикс домена;

     SQLServerPort – порт SQL-сервера, определенный в п. 2.

Добавлять и удалять имена SPN может только администратор домена. Просматривать список зарегистрированных имен SPN может любой доменный пользователь.

Настройка доверия делегирования служб Kerberos

1. На контроллере домена запустите оснастку «Active Directory – Пользователи и компьютеры».
2. В свойствах учетной записи пользователя, от имени которого работает пул приложений NOMAD, на закладке «Делегирование»:
   - установите переключатели **Доверять этому пользователю делегирование указанных служб** и **Использовать любой протокол проверки подлинности**:



   - выберите службу, для которой нужно настроить делегирование. Для этого:
     a) Последовательно нажмите на кнопки **Добавить...**, **Пользователи и компьютеры**.
     b) В открывшемся окне с помощью поиска найдите и выберите пользователя или компьютер, для которого настроено имя SPN. Нажмите на кнопку **ОК**.
     c) В списке служб выберите запись **MSSQLSvc**, напротив которой указан порт SQL-сервера с базой данных DIRECTUM.
     d) Последовательно нажмите на кнопки **ОК** и **Применить**.

Настройка в приложении DIRECTUM Solo и DIRECTUM Jazz для iOS

1. С помощью приложения iTunes добавьте закрытый ключ сертификата, используемого для аутентификации, в папку «Документы» приложения DIRECTUM Solo или DIRECTUM Jazz.
2. На странице аутентификации нажмите на кнопку **По сертификату** и в списке сертификатов выберите добавленный сертификат.

Настройка в приложении DIRECTUM Solo и DIRECTUM Jazz для Android

1. В настройках устройства в разделе «Безопасность» задайте PIN-код, пароль или графический ключ для блокировки экрана.
2. Скопируйте на устройство пользовательский сертификат (*.pfx или *.p12) и сертификат центра сертификации.
3. Последовательно выберите **Настройки**/**Безопасность** и установите оба сертификата:
   a) В настройках профиля **Сертификаты/Настройка RSA-сертификатов** нажмите на кнопку **Импортировать сертификаты в локальное хранилище**.
   b) Добавьте необходимые сертификаты. Для каждого сертификата при добавлении введите пин-код и нажмите на кнопку **Добавить**.
4. На странице аутентификации нажмите на кнопку **По сертификату**. В открывшемся окне выберите пользовательский сертификат и нажмите на кнопку **Разрешить**.

   Пример выбора сертификата в приложении DIRECTUM Jazz: