Интеграция Microsoft PKI

В данной статье описана быстрая настройка Microsoft PKI с помощью AxelNAC.

Общие сведения

Для иллюстрации интеграции AxelNAC с Microsoft PKI приняты следующие допущения:

1. Имеется как минимум один сервер с AxelNAC 0.8 или более поздней версии.
2. К AxelNAC уже подключен правильно настроенный коммутатор или точка доступа с поддержкой 802.1X.
3. Сервер AxelNAC RADIUS работает в существующей среде.
4. Установлен сервер Microsoft Windows Server 2016.
5. IP-адрес управления AxelNAC — 192.168.1.5.
6. Общая секретная фраза RADIUS — useStrongerSecret.
7. Описаны разные случаи использования **<ServerDNSName>**, большинство сервисов MSPKI требует в своей конфигурации использовать FQDN сервера, а не его IP-адрес.

Установка Microsoft PKI

Установка службы сертификатов Active Directory (ADCS)

В данной секции рассматривается настройка служб сертификации Active Directory Certificate Services в Microsoft Windows Server 2016. Установка ADCS не описывается (информация об этом приведена в официальной документации Microsoft).

Для интеграции с AxelNAC в ADCS должны быть установлены следующие подпрограммы:

- Certification Authority Web Enrollment
- Network Device Enrollment Service
- Online Responder

Перед настройкой может понадобиться установить исправление, связанное с проблемой Microsoft. После перезапуска службы ADCS сервер не сможет зарегистрировать новые сертификаты и будет выдавать следующее сообщение об ошибке: RPC Server is unavailable. Исправление доступно по ссылке.

Связь между MSPKI и AxelNAC будет осуществляться через порт 80.

Настройка службы регистрации сетевых устройств (NDES)

Для развертывания ADCS необходимо настроить службу Network Device Enrollment Service (NDES). Эта позволит обмениваться сертификатами с сервером MSPKI по протоколу Simple Certificate Exchange Protocol (SCEP).

Каждое изменение конфигурации должно выполняться учетной записью с правами администратора.

Пароль вызова

Microsoft SCEP (MSCEP) по умолчанию включает в себя пароль вызова, который является уникальным и динамически генерируется для каждого устройства, желающего зарегистрироваться. В условиях BYOD это может стать препятствием, поскольку пользователь не может зарегистрировать устройство самостоятельно без вмешательства администратора. Поскольку NDES используется вместе с AxelNAC, то для получения сертификата потребуются учетные данные, необходимые для доступа к системе регистрации.

Для отключения пароля вызова необходимо изменить ключ в реестре Windows. Для этого выполните следующие действия:

Шаг 1. Нажмите кнопку **Start** и введите **regedit**.

Шаг 2. Перейдите в раздел **Computer → HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Cryptography → MSCEP → EnforcePassword** и поменяйте значение параметра **EnforcePassword** на 0 (значение по умолчанию 1).

Увеличение длины URL-адреса для запроса

Рекомендуется увеличивать длину URL, чтобы избежать проблем с длинными запросами. Для этого введите следующую команду в CLI на сервере NDES:

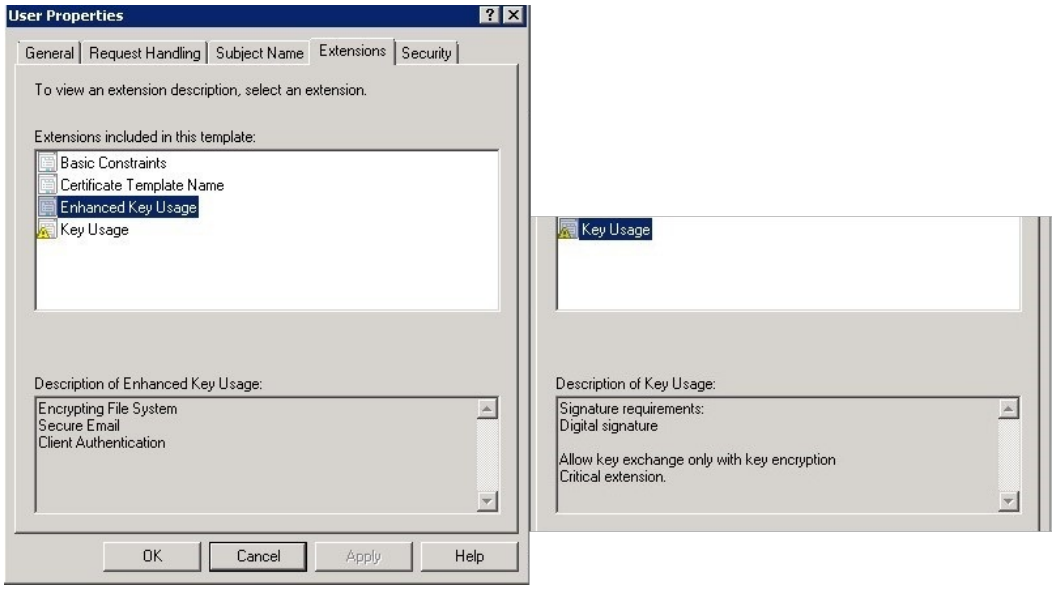
%systemroot%system32inetsrvappcmd.exe set config /section:system.webServer/ security/requestFiltering /requestLimits.maxQueryString: "16384" /commit:apphost

Шаблон сертификата

Недействительность вашего центра сертификации может повлиять на всю архитектуру сертификатов.

Предоставление сертификатов для аутентификации пользователей является важной целью, поэтому необходимо настроить специальный шаблон.

Во-первых, шаблон сертификата должен содержать как минимум следующие параметры **Enhanced Key Usage** и **Key Usage**:



Следующий этап — дублирование шаблона, в котором уже настроены параметры **Key Usage** и **Enhanced Key Usage**. Рекомендуется продублировать шаблон **User** и изменить настройки.

Для этого, выполните следующие действия:

Шаг 1. Продублируйте шаблон. Перейдите в **Server Manager → Roles → Active Directory Certificates Services → Certificate templates** , щелкните правой кнопкой мыши на шаблоне **User** и выберите **Duplicate this template**.

Шаг 2. Кликните правой кнопкой мыши на новом шаблоне и перейдите в раздел **Properties**. На вкладке **Subject Name** убедитесь, что в запросе выбрано значение **Supplied**, а не **Built from information in Active Directory** , иначе NDES перезапишет запрошенный CN.

Шаг 3. Разрешите NDES использовать этот шаблон. Перейдите в раздел **Server Manager → Roles → Active Directory Certificates Services** и разверните параметр **<ServerDNSName>**.

Шаг 4. Кликните правой кнопкой мыши на шаблоне сертификата и выберите **New template to issue**, затем выберите в списке только что созданный шаблон.

Шаг 5. Настройте в реестре выбранный шаблон. Для доступа к редактору реестра нажмите кнопку **Start** и введите **regedit**.

Шаг 6. В реестре перейдите в раздел **Computer → HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Cryptography → MSCEP** . Должен появиться список из трех ключевых записей:

- EncryptionTemplate,
- GeneralPurposeTemplate,
- SignatureTemplate.

Шаг 7. Замените каждое значение именем вновь созданного шаблона.

Шаг 8. Перезагрузите NDES-сервер, чтобы применить изменения в реестре.

Конфигурация IIS

Использование SCEP с AxelNAC также требует внесения изменений в конфигурацию IIS:

Шаг 1. Перейдите в раздел **Server Manager → Web(IIS)**.

Шаг 2. Раскройте элемент **Default web site** и выберите **CertSrv → mscep**.

Шаг 3. Выберите **Authentication** и дважды кликните на значении **Anonymous Authentication**.

Шаг 4. Убедитесь, что выбран идентификатор пула приложений.

Online Certificate Status Protocol (OCSP)

Для настройки OCSP необходимо внести следующие изменения:

Шаг 1. Разрешите серверу использовать шаблон **OCSPResponseSigning** сервером. Перейдите в раздел **Server Manager → Roles → Active Directory Certificates Services**, раскройте параметр **<ServerDNSName>**, кликните правой кнопкой мыши на **Certificate template** и выберите **New template to issue**. Затем, в списке выберите **OCSPResponseSigning**.

Шаг 2. После установки OCSP создайте конфигурацию отзыва. Перейдите в раздел **Server Manager → Roles → Active Directory Certificate Services** , раскройте параметр **OnlineResponder: <ServerDNSName>**, кликните правой кнопкой мыши на **Revocation Configuration** и выберите **Add Revocation Configuration**. Затем нажмите **Next**.

Шаг 3. Выберите имя конфигурации и нажмите Next.

Шаг 4. Выберите значение **Select a certificate for an existing enterprise CA** и нажмите **Next**.

Шаг 5. Нажмите кнопку **Browse**. Найдите в списке корпоративный центр сертификации, выберите его, нажмите **OK** и затем **Next**.

Шаг 6. Укажите автоматический выбор сертификата подписи: **Automatically select a signing certificate**. Убедитесь, что выбрана опция автоматической регистрации **Auto-Enroll for an OCSP signing certificate**.

Шаг 7. В раскрывающемся списке рядом с **Certificate Template** выберите шаблон OCSP по умолчанию **OCSPResponseSigning**. Добавлять провайдеров нужно только в том случае, если помимо OCSP нужно использовать CRL.

Шаг 8. После создания конфигурации, кликните правой кнопкой мыши на конфигурации отзыва и выберите **Edit properties**.

Шаг 9. Перейдите на вкладку **Signing** и выберите **Enable NONCE extension support**, затем нажмите **OK**.

Шаг 10. Убедитесь, что OCSP-сервер появился в настройках центра сертификации. Кликните правой кнопкой мыши на центре сертификации и

выберите **Properties**. Перейдите на вкладку **Extension** и в раскрывающемся списке **Select extension** выберите значение **Authority Information Access (AIA)**.

Шаг 11. Убедитесь, что в списке расположений есть следующее значение:

http://<DNS-имя_СЕРВЕРА>/OCSP.

Если этого адреса нет, добавьте его с помощью кнопки **Add...** В открывшемся меню введите **http://**, затем вставьте **<DNS-имя_СЕРВЕРА>** и введите **/OCSP**, затем нажмите **OK**.

Шаг 12. Убедитесь, что выбрано расширение **Include in the online certificate status protocol(OCSP)** . По умолчанию OCSP имеет двухдневную задержку обновления информации в CRL. Это означает, что AxelNAC обнаружит отзыв сертификата только через два дня.

Шаг 13. Задержку можно изменить на сервере NDES. Для этого перейдите в раздел **Server Manager → Roles → Active Directory Certificate Service** , кликните правой кнопкой мыши на **Enterprise PKI** и выберите **Options...**.

Шаг 14. Поменяйте значение параметра **Set CRL status to Expiring when expiring in:** на нужное значение задержки.

Генерация сертификатов RADIUS

Использование Microsoft PKI предполагает, что все сертификаты будут поставляться корневым центром сертификации MSPKI. Для аутентификации RADIUS потребуется сгенерировать сертификат для AxelNAC. Для генерации сертификата RADIUS будет использоваться шаблон WebServer. Выполните следующие действия:

Шаг 1. Создайте запрос (CSR) закрытого ключа с сервера AxelNAC и отправьте CSR на сервер NDES. Подключитесь к контроллеру через SSH и введите в CLI следующие команды для создания CSR и подписания его закрытым ключом:

openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr

Будет предложено ввести информацию. Пример правильной конфигурации:

- CN=AxelNAC.local;
- C=CA;
- ST=QC;
- Locality=Moscow;
- Organization=Имя_организации;
- Organization Unit=IT.

Все поля, кроме CN, не обязательны для заполнения.

Для аутентификации сервера AxelNAC необходимо выпустить один сертификат, который будет использоваться для всех узлов. CN в сертификате, выпущенном для сервера, может иметь любое значение.

Шаг 2. После получения CSR отправьте его на сервер NDES. Скопируйте содержимое запроса (CSR) на сайте регистрации МСПКИ для ввода запроса. URL для ввода запроса: **http://<DNS-имя_СЕРВЕРА>/CertSrv/**.

Шаг 3. На открывшейся странице нажмите **Request a certificate** и выберите значение **advanced certificate request**.

Шаг 4. Вставьте содержимое CSR-файла и выберите шаблон **Web Server**, после чего нажмите **Submit**.

Шаг 5. В качестве метода шифрования выберите **Base 64 encoded** и нажмите **Download certificate**. В результате пользователь получит сертификат (открытый ключ) для AxelNAC.

Шаг 6. Загрузите файл CA в браузере по следующему URL: **http://<DNS-имя_СЕРВЕРА>/CertSrv**. Нажмите кнопку для загрузки сертификата ЦС, цепочки сертификатов или CRL: **Download a CA certificate, certificate chain or CRL** .

Шаг 7. Выберите сертификат ЦС в списке.

Шаг 8. Выберите **Base 64** в качестве метода шифрования и загрузите сертификат ЦС, нажав **Download CA certificate**.

Шаг 9. Скопируйте эти файлы в AxelNAC.

Настройка AxelNAC

Установка сертификата сервера в AxelNAC

Перед выполнением следующих шагов убедитесь, что при выпуске сертификата был установлен параметр "**аутентификация сервера**" для EKU (Extended Key Usage).

Для того, чтобы сконфигурировать соединение с аутентификацией по протоколу EAP-TLS необходимо установить сертификаты на сервере AxelNAC. Поля, которые могут содержать сертификаты показаны в таблице ниже.

Обязательные и опциональные поля сертификатов

Поле	Описание	Пример	Статус
UPN	User Principal Name пользователя	nb1@axeldemo.pro	Для выполнения аутентификации необходимо заполнить хотя бы одно из этих полей
CN	Common Name пользователя	nb1@axeldemo.pro	
DNS	DNS APM	nb1.axeldemo.pro	
IP Address	IP-адрес APM	192.31.205.15	Данные поля носят информационный характер и не требуют заполнения
Street Address	Географический адрес APM	ul. Lenina, 9A	
State or Province	Область/провинция/штат, для которого действителен сертификат	Mockovskaya oblast	
Country	Страна, для которой действителен сертификат	Honolulu	
Organizational Unit	Подразделение, для которого действителен сертификат	HR	
Organization	Организация, для которой действителен сертификат	AxelPRO	

Шаг 1. Перейдите на вкладку RADUIS в разделе **Конфигурация → Настройки системы → SSL-сертификаты** и нажмите на кнопку **Редактировать**.

Шаг 2. На открывшейся странице замените предустановленные данные в полях **Сертификат сервера RADIUS**, **Закрытый ключ сервера RADIUS** и **Сертификат(ы) центра сертификации** данными, полученными в ЦС и нажмите **Сохранить** в левом нижнем углу страницы.

После установки SSL-сертификата вам будет предложено перезапустить сервис **radiusd-auth**. Вы можете пропустить этот шаг, т.к. данный сервис, в любом случае, нужно будет перезапустить после окончательной настройки соединения.

Шаг 3. Перейдите в раздел **Конфигурация → Настройки системы → RADUIS → SSL-сертификаты PKI** и нажмите на кнопку **Новый SSL-сертификат**.

Шаг 4. На открывшейся странице заполните поля следующим образом:

- **Идентификатор** — введите имя профиля;
- **Сертификат** — укажите сертификат, выпущенный ЦС для сервера;
- **Центр сертификации** — укажите сертификат удостоверяющего центра;
- **Закрытый ключ** — укажите закрытый ключ сертификата;
- **Пароль для закрытого ключа** — укажите пароль для контейнера сертификатов (при наличии);
- **Сертификат(ы) промежуточного центра сертификации (CA)** — при наличии промежуточного центра сертификации необходимо указать его сертификат, в ином случае, укажите сертификат удостоверяющего центра.

После этого, нажмите **Создать** в левом нижнем углу страницы.

Шаг 5. Перейдите на вкладку **Профили TLS** и нажмите **Новый TLS-профиль**.

Шаг 6. На открывшейся странице заполните поля следующим образом:

- **Идентификатор** — введите имя профиля;
- **Профиль сертификата** — укажите имя SSL-профиля созданного в предыдущем шаге;
- **Минимальная версия TLS** — минимальная версия TLS, поддерживаемая подключаемыми устройствами;
- **Максимальная версия TLS** — максимальная версия TLS, поддерживаемая подключаемыми устройствами.

Мы рекомендуем выбирать минимальную версию TLS 1.2 и максимальную — 1.3, т.к. эти версии являются самыми актуальными.

После этого, нажмите **Создать** в левом нижнем углу страницы.

Шаг 7. Перейдите на вкладку **Профили EAP** и нажмите **Новый профиль EAP**.

Шаг 8. На открывшейся странице заполните поля следующим образом:

- **Идентификатор** — введите имя профиля;
- **Тип EAP по умолчанию** — TLS;
- **Типы EAP-аутентификации** — TLS;
- **Профиль TLS** — укажите имя TLS-профиля созданного в предыдущем шаге.

После этого, нажмите **Создать** в левом нижнем углу страницы.

Шаг 9. Перезапустите сервис **radiusd-auth**.

Перезагрузка данной службы может привести к таймауту текущих RADIUS-сессий аутентификации.

Конфигурация провайдера PKI в AxelNAC

Для использования PKI необходимо произвести конфигурацию провайдера в веб-интерфейсе AxelNAC. Конфигурация провайдера определяет, как AxelNAC подключается к MSPKI и какая информация будет передаваться. Для этого выполните следующие действия:
Шаг 1. Перейдите в раздел **Конфигурация → Расширенные настройки доступа → PKI-провайдеры** , нажмите **Новый PKI-провайдер** и в выпадающем списке выберите значение **SCEP**.

Шаг 2. Заполните форму для провайдера PKI в соответствии с конфигурацией центра сертификации.

Для URL Не используйте протокол **https:**.

- Для такой конфигурации не требуется комбинация логина и пароля (Имя пользователя/Пароль).
- В значениях параметров **Файл сертификата CA** и **Файл сертификата сервера** должны быть указаны абсолютные пути к файлам сертификатов. Пример абсолютного пути: **/usr/local/pf/conf/ssl/tls_certs/MyCA.pem**
- Параметр **Атрибут общего имени** определяет, как будет генерироваться сертификат и какой тип «владельца» будет связывать сертификат с подключением. Если выбрать значение **MAC-адрес**, то сертификат будет сгенерирован с использованием MAC-адреса в качестве идентификатора. Если выбрать значение **Имя пользователя**, то сертификат будет сгенерирован с использованием имени пользователя на сервере аутентификации.

Конфигурация агентов инициализации

Агенты инициализации позволяют устройствам автоматически настраивать подключение к соответствующему SSID (если применимо), использовать соответствующий метод аутентификации (например, EAP-TLS) и доверять сертификату ЦС и любому подписанному им сертификату. Подробный процесс настройки агентов инициализации описан в разделе Интеграция с агентами инициализации.

Отладка интеграции MSPKI с AxelNAC

Для того, чтобы провести процедуру регистрации вручную, для отладочных целей, выполните следующие действия:

Шаг 1. Сгенерируйте запрос и его закрытый ключ с помощью команды openssl. Введите следующие команды в AxelNAC CLI:

```
mkdir temp; cd temp
openssl req -newkey rsa:2048 -nodes -keyout local.key -out local.csr -subj
'/C=CA/ST=Moscow/L=Mytishi/O=Reverse/OU=IT/CN=www.test.example.ru'
```

В результате в этом каталоге будут созданы два файла: **local.csr** и **local.key**.

Шаг 2. Получите сертификат ЦС и специфические сертификаты из MSPKI с помощью команды:

```
sscep getca -u http://<DNS-имя_СЕРВЕРА>/CertSrv/mscep/ -c MyCA.crt
```

Шаг 3. Используйте сертификаты **CEP encryption** и **Enrollment agent**. Оба сертификата были получены при выполнении команды sscep getca. Должно быть, как минимум, три сертификата с одинаковым именем и разными цифрами в конце: например, **MyCA.crt-0** (сертификат агента регистрации), **MyCA.crt-1** (сертификат шифрования CEP) и **MyCA.crt-2** (сертификат ЦС). Для отображения содержимого каждого сертификата используйте следующие команды:

```
openssl x509 -in MyCA.crt-0 —text
openssl x509 -in MyCA.crt-1 —text
openssl x509 -in MyCA.crt-2 —text
```

Шаг 4. В результатах поиска найдите расширение X509v3.

Шаг 5. Используйте команду sscep enroll:

sscep enroll -c MyCA.crt-0 -e MyCA.crt-1 -k local.key -r local.csr
-l MyCert.crt -S sha1 -u http://<DNS-имя_СЕРВЕРА>/CertSrv/mscep/ -d

При использовании этой команды в качестве аргумента для **-c** потребуется сертификат агента **Enrollment agent**, а в качестве аргумента для **-e** — сертификат шифрования **CEP Encryption**. параметр **-d** используется для вывода отладочной информации. **-l** — локальный файл, в котором будет сохранен сертификат.

Шаг 6. Для проверки сертификата по OCSP можно использовать следующую команду openssl:

openssl OCSP -issuer path/CA-Certificate -cert path/Certificate-to-verify -text -url http://<DNS-имя_СЕРВЕРА>/OCSP

Отладка Passthrough в Android

Если в **Passthrough** необходимо добавить домены, предлагается перехватить трафик, идущий с устройства, которое не может получить доступ к Google Play Store. Для этого можно использовать, например, команду tcpdump, получить IP-адрес устройства и выполнить в AxelNAC CLI следующую команду:

tcpdump -i $REGISTRATION_INTERFACE -n dst port 53 and src host @IP-АДРЕС_УСТРОЙСТВА

В результате все DNS-запросы с устройства будут передаваться в AxelNAC. Нужно будет найти связанный с Google домен и добавить его в список **Passthrough**.

ID статьи: 353
Последнее обновление: 24 окт., 2024
Обновлено от: Егоров В.
Ревизия: 5
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.2.0 -> AxelNAC. Руководство администратора -> Интеграция PKI -> Интеграция Microsoft PKI
https://docs.axel.pro/entry/353/