Проблема аутентификации ovirt-provider-ovn на engine SSO

1. Проблема

После замены сертификата веб-портала не работает раздел управляемых сетей (**Сеть > Управляемые сети**), не отображаются сети и другие сущности, не создаются новые сети, возникает ошибка:

```
Ошибка создания сети: "Внутрисистемная ошибка при получении списка логических
сетей: HTTPSConnectionPool(host='engine.local', port=443): Max retries exceeded
with url: /ovirt-engine/sso/oauth/token-info (Caused by SSLError(SSLError(1,
'[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:897)'),))"
```

В логах сервиса ovirt-provider-ovn присутствуют следующие события:

```
root HTTPSConnectionPool(host='engine.local', port=443): Max retries exceeded
with url: /ovirt-engine/sso/oauth/token-info (Caused by SSLError(SSLError(1,
'[SSL: CERTI FICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:897)'),))

Traceback (most recent call last):
    File "/usr/lib/python3.6/site-packages/urllib3/connectionpool.py", line 600,
in urlopen     chunked=chunked)
    File "/usr/lib/python3.6/site-packages/urllib3/connectionpool.py", line 343,
in _make_request self._validate_conn(conn)
    File "/usr/lib/python3.6/site-packages/urllib3/connectionpool.py", line 839,
in _validate_conn     conn.connect()
    File "/usr/lib/python3.6/site-packages/urllib3/connection.py", line 358, in
connect     ssl_context=context)
    File "/usr/lib/python3.6/site-packages/urllib3/util/ssl_.py", line 354, in
ssl_wrap_socket return context.wrap_socket(sock,
server_hostname=server_hostname)
    File "/usr/lib64/python3.6/ssl.py", line 365, in wrap_socket _context=self,
_session=session)
    File "/usr/lib64/python3.6/ssl.py", line 776, in __init__
self.do_handshake()
    File "/usr/lib64/python3.6/ssl.py", line 1036, in do_handshake
self._sslobj.do_handshake()
    File "/usr/lib64/python3.6/ssl.py", line 648, in do_handshake
self._sslobj.do_handshake()

ssl.SSLError: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed
(_ssl.c:897)
```

2. Решение

Проблема возникает, если сертификат веб-портала подписан промежуточным CA-сертификатом и в файле **/etc/pki/ovirt-engine/apache-ca.pem** отсутствует полная цепочка до корневого CA-сертификата.

Для решения проблемы необходимо скомпоновать файл **/etc/pki/ovirt-engine/apache-ca.pem** согласно инструкции (цепочка сертификатов должна заканчиваться корневым самоподписанным сертификатом) и выполнить перезапуск сервиса **httpd**:

```
systemctl restart httpd
```

Обновление сертификата libvirt

Аннотация

Статья рассматривает обновление сертификата **libvirt** с истекшим сроком действия.

При истечении срока действия данного сертификата невозможна миграция ВМ, необходимая для того, чтобы зарегистрировать сертификат хоста

1. Процедура обновления

Проверьте на менеджере управления, посылает ли хост запрос на подпись. Для этого убедитесь в наличии файла по пути **/etc/pki/ovirt-engine/requests-qemu/<Host_FQDN_OR_IP>.req**.

На хосте введите команду для отображения значения **subject** старого сертификата:

```
openssl x509 -in /etc/pki/vdsm/libvirt-migrate/server-cert.pem  -noout -subject
subject=O = example.com, OU = qemu, CN = host.example.com
```

На менеджере управления подпишите запрос:

```
/usr/share/ovirt-engine/bin/pki-enroll-request.sh \
        --name=host.example.com \ ①
        --subject="/O=example.com/OU=qemu/CN=host.example.com" \ ②
        --san="DNS:host.example.com" \ ③
        --days=3650 \
        --ca-file=qemu-ca  \
        --cert-dir=certs-qemu \
        --req-dir=requests-qemu
```

① - замените `host.example.com` на имя хоста, полученное из `CN` в выводе предыдущей команды.

② - замените `example.com` и `host.example.com` на имена организации и хоста, полученные из `O` и `CN` в выводе предыдущей команды.

③ - замените на значение, полученное из `CN` в выводе предыдущей команды.

- Если хост идентифицируется по FQDN, тогда используйте формат `DNS:<host-fqdn>`, например, `DNS:host.example.com`.
- Если хост идентифицируется по IP, тогда используйте формат `IP:<host-ip>`, например, `IP:1.2.3.4`.

Скопируйте сгенерированный сертификат на хост:

```
scp -i /etc/pki/ovirt-engine/keys/engine_id_rsa /etc/pki/ovirt-engine/certs-qemu/host.example.com.cer root@host.example.com:/etc/pki/vdsm/libvirt-migrate/server-cert.pem
```

Временно отключите управление питанием на хосте и перезапустите службу **libvirtd**:

```
systemctl restart libvirtd
```

Обновление SSL сертификата на хостах и менеджере управления

Аннотация

Статья рассматривает обновление сертификатов, выпущенных средой виртуализации zVirt

> Сертификаты, выпущенные сторонними центрами сертификации не используются внутренними службами среды виртуализации. Сертификаты сторонних центров применяются только для веб-интерфейса.

1. Обновление сертификатов служб хостов виртуализации, срок действия которых еще не окончился.

Обновление производится с помощью веб-интерфейса менеджера управления. Для это выполните следующие шаги:

1. На портале администрирования перейдите в **Ресурсы > Хосты**
2. Выделите нужный для обновления хост и переведите его в режим обслуживания: **[Управление]** > **[Обслуживание]**
3. После перехода хоста в режим обслуживания нажмите **[Настройки]** > **[Регистрация сертификата]**.
4. После установки сертификата, активируйте хост. Выбрать `Управление > Включить`.

2. Обновление сертификатов менеджера управления.

В режиме Standalone

1. Подключитесь по SSH или через Cockpit к хосту с менеджером управления под учетной записью *root*.
2. Запустите команду настройки Менеджера управления:

```
engine-setup --offline
```

3. Ответьте на вопросы или используйте файл ответов

> В версии zVirt 3.3 и старше обязательно ответьте **Yes** на вопрос о перевыпуске сертификата.

В режиме HostedEngine

1. Подключитесь по SSH или через Cockpit к хосту, на котором работает ВМ HostedEngine и активируйте режим глобального обслуживания.

```
hosted-engine --set-maintenance --mode=global
```

2. Подключитесь по SSH или через Cockpit к ВМ HostedEngine под учетной записью *root*.
3. Запустите команду настройки Менеджера управления:

```
engine-setup --offline
```

4. Ответьте на вопросы или используйте файл ответов.

> В версии zVirt 3.3 и старше обязательно ответьте **Yes** на вопрос о перевыпуске сертификата.

5. После окончания процедуры настройки Менеджера, с хоста, на котором работает ВМ HostedEngine, отключите режим глобального обслуживания.

```
hosted-engine --set-maintenance --mode=none
```

3. Возможные ошибки на менеджере управления при обновлении сертификата.

3.1. Ошибка Old AdminPassword found in vdc_options

Полный текст ошибки:

```
Old AdminPassword found in vdc_options. This should not happen, and is likely a
result of a bad past upgrade.
Please contact support.
```

Для устранения:

1. Выполните команду:

```
/usr/share/ovirt-engine/dbscripts/engine-psql.sh -c \
            "select fn_db_delete_config_value('AdminPassword','general');"
```

2. Повторно запустите команду настройки Менеджера:

```
engine-setup --offline
```

3.2. Не обновляются некоторые сертификаты

Проблема с сертификатами:

```
/etc/pki/ovirt-engine/certs/ovirt-provider-ovn Apr 6 11:47:13 2023 GMT
/etc/pki/ovirt-engine/certs/ovn-ndb.cer Apr 6 11:47:12 2023 GMT
/etc/pki/ovirt-engine/certs/ovn-sdb.cer Apr 6 11:47:12 2023 GMT
/etc/pki/ovirt-engine/certs/vmconsole-proxy-helper.cer Apr 6 11:47:12 2023 GMT
/etc/pki/ovirt-engine/certs/vmconsole-proxy-host.cer   Apr 6 11:47:12 2023 GMT
/etc/pki/ovirt-engine/certs/vmconsole-proxy-user.cer   Apr 6 11:47:13 2023 GMT
```

Все указанные сертификаты можно обновить с помощью команд:

BASH

```
/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh --name="ovirt-provider-ovn" --
password=mypass --subject="/C=US/O=example.com/CN=FQDN имя вашего менеджера" --
keep-key

/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh --name="ovn-ndb" --
password=mypass --subject="/C=US/O=example.com/CN=FQDN имя вашего менеджера" --
keep-key

/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh --name="ovn-sdb" --
password=mypass --subject="/C=US/O=example.com/CN=FQDN имя вашего менеджера" --
keep-key

/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh --name="vmconsole-proxy-helper"
--password=mypass --subject="/C=US/O=example.com/CN=FQDN имя вашего менеджера" -
-keep-key

/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh --name="vmconsole-proxy-host" -
-password=mypass --subject="/C=US/O=example.com/CN=FQDN имя вашего менеджера" --
keep-key

/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh --name="vmconsole-proxy-user" -
-password=mypass --subject="/C=US/O=example.com/CN=FQDN имя вашего менеджера" --
keep-key

systemctl restart ovirt-provider-ovn.service

systemctl restart ovn-northd.service
```

Строка `--password=mypass` должна быть именно такой, не нужно писать ваш пароль.

3.3. Ошибка ovsdb-server.service

Ошибка в логах:

```
Dec nn nn:nn:nn FQDN.server ovsdb-server[895684]: ovs|07062|jsonrpc|WARN|ssl:
[::ffff:10.31.131.14]:57818: receive error: Protocol error
Dec nn nn:nn:nn FQDN.server ovsdb-server[895684]: ovs|07063|reconnect|WARN|ssl:
[::ffff:10.31.131.14]:57818: connection dropped (Protocol error)
Dec nn nn:nn:nn FQDN.server ovsdb-server[895684]:
ovs|07064|stream_ssl|WARN|SSL_accept: error:1417C086:SSL
routines:tls_process_client_certificate:certificate verify failed
```

Решение - перезагрузить ovsdb-server.service на Менеджере Управления и на Хостах:

```
systemctl restart ovsdb-server.service
```

Решение проблемы с сертификатами Libvirt описано в статье, доступной по ссылке

Обновление просроченного SSL сертификата на хосте

1. Проблема

SSL сертификат на хосте просрочен, статус хоста `Not Responding`. Нет возможности управлять ВМ, запущенными на этом хосте с помощью менеджера управления.

2. Решение

Следующие шаги необходимо проводить только для хостов, находящихся в статусе `not responding`.

Чтобы обновить сертификат на хосте необходимо проделать следующее:

1. Скопировать файл с ключом `vdsmkey.pem` на менеджер управления:

```
scp /etc/pki/vdsm/keys/vdsmkey.pem root@<RFQDN OR IP>:/tmp/vdsmkey.pem
```

2. На менеджере сделать зашифрованный запрос на выпуск сертификата, используйте ключ (**pass:mypass не менять!**):

```
openssl req -new -key /tmp/vdsmkey.pem -out /tmp/test_host_vdsm.csr -passin "pass:mypass" -passout "pass:mypass" -batch -subj "/"
```

3. На хосте выполнить команду для вывода `subject` старого сертификата:

```
openssl x509 -in /etc/pki/vdsm/certs/vdsmcert.pem -noout -subject
```

4. На менеджере подписать сертификат, используя Engine CA. В параметр `subj ` вставить вывод из предыдущей команды, выполненной на хосте.

```
cd /etc/pki/ovirt-engine/
```

```
openssl ca -batch -policy policy_match -config openssl.conf -cert ca.pem -keyfile  private/ca.pem -days +398 -in  /tmp/test_host_vdsm.csr -out /tmp/test_host_vdsm.cer -startdate "$(date --utc --date "now -1 days" +"%y%m%d%H%M%SZ")" -subj "/O=Test/CN=test.com" -utf8
```

5. Скопировать с менеджера подписанный сертификат обратно на хост `/etc/pki/vdsm/certs/vdsmcert.pem`.

```
scp /tmp/test_host_vdsm.cer root@<FQDN OR
IP>:/etc/pki/vdsm/certs/vdsmcert.pem
```

6. На хосте скопировать сертификат в ` libvirt `.

```
cp /etc/pki/vdsm/certs/vdsmcert.pem /etc/pki/vdsm/libvirt-spice/server-
cert.pem
cp /etc/pki/vdsm/certs/vdsmcert.pem /etc/pki/vdsm/libvirt-vnc/server-
cert.pem
cp /etc/pki/vdsm/certs/vdsmcert.pem /etc/pki/libvirt/clientcert.pem
```

7. Временно отключить менеджер питания хоста.
8. Перезапустить службы `libvirt` и `vdsmd`. Дождаться пока хост не перейдет в статус `Up`.

```
systemctl restart libvirtd.service
systemctl restart vdsmd.service
```

Возможно, что сертификаты `libvirt-migrate` также были просрочены. Необходимо воспользоваться инструкцией по обновлению сертификата libvirt.

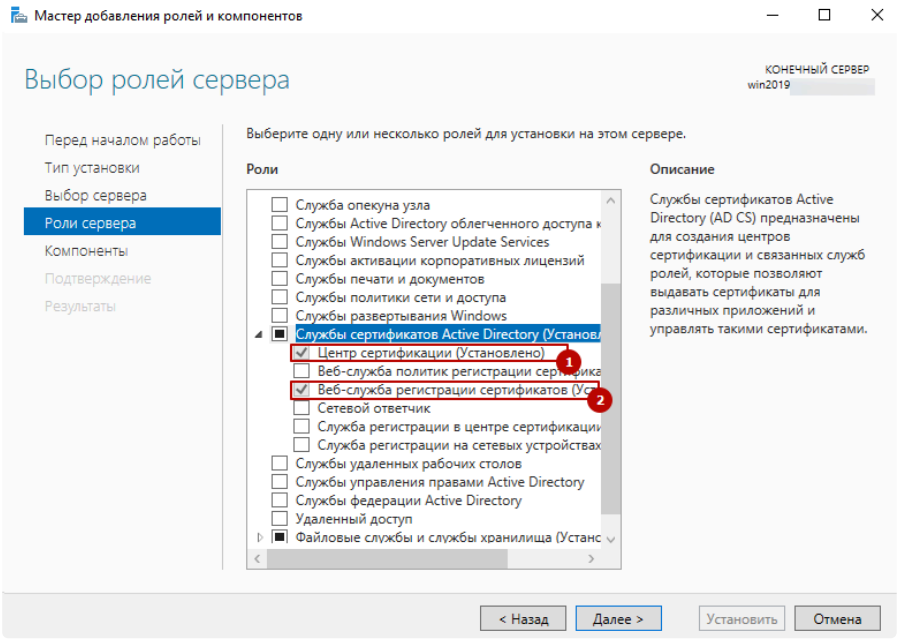
Выпуск самоподписанного SSL сертификата в ЦС Windows Server для менеджера управления zVirt

1. Подготовка ЦС на базе роли Windows Server "Службы сертификатов Active Directory"

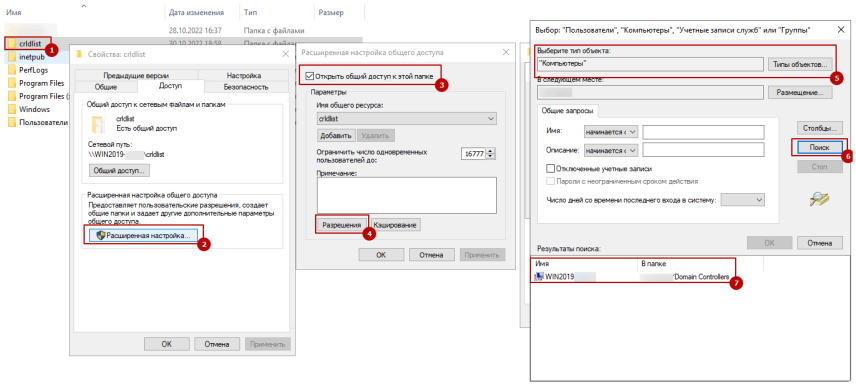
Данная инструкция описывает последовательность действий для выпуска и последующей замены сертификата по инструкции

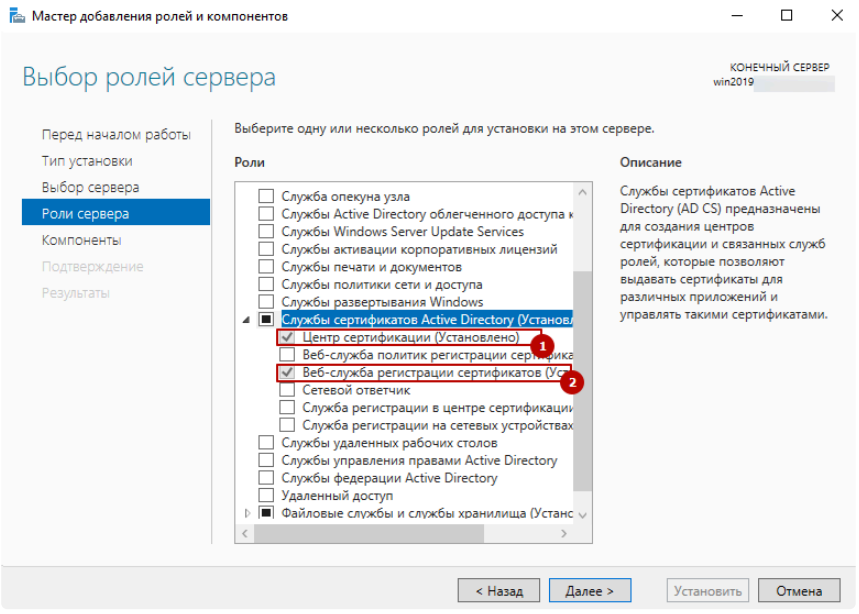
2. Установка ролей

1. Установить роль **Службы сертификатов Active Directory**: **Центр сертификации** и **Веб-служба регистрации сертификатов** Инструкция на сайте Microsoft.

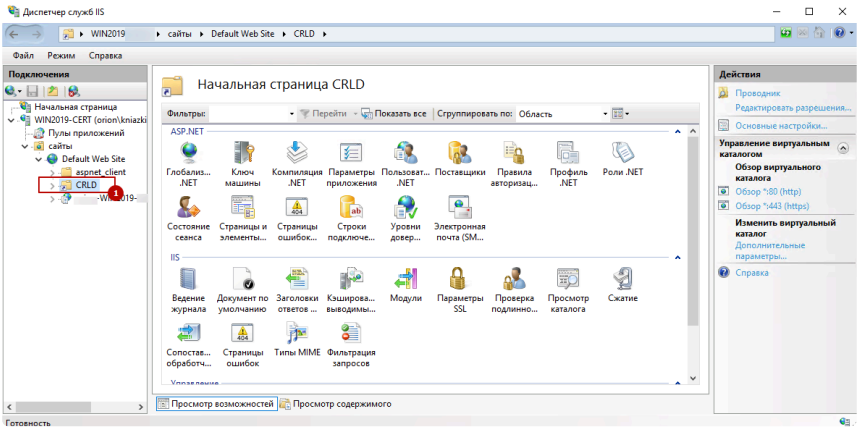


2. Установить роль **Веб сервер IIS** с предложенными по умолчанию компонентами и произвести настройку. Для этого:.
    - На диске C создать папку с именем **rldlist**. Например **C:\crldlist**.
    - Предоставить общий сетевой доступ к папке, настроить текущей для учетной записи "Компьютер" полный доступ.

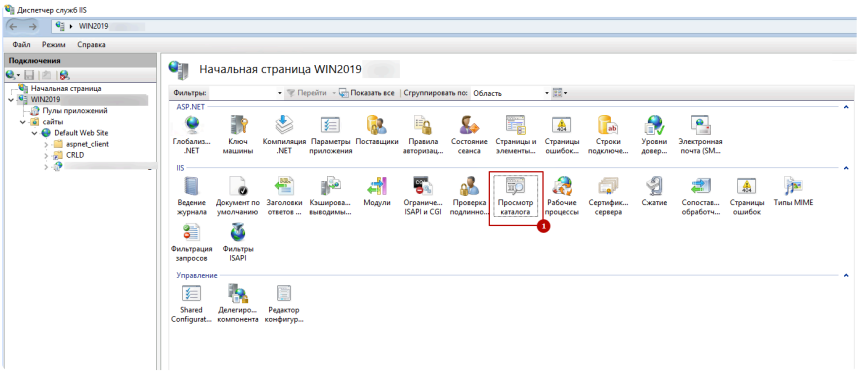


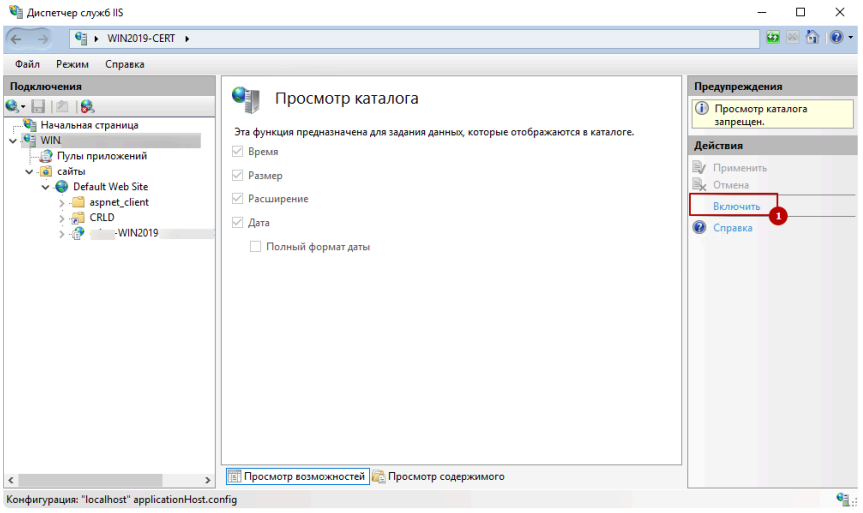


- Подключиться к **Диспетчеру служб IIS** , выбрать **имя сервера > Сайты > Default Web Site > ПКМ - Добавить виртуальный каталог**. В поле **Псевдоним** вписать имя **CRLD**, в поле **Физический путь** указать путь до созданной на предыдущем шаге папки, например **C:\crldlist**.

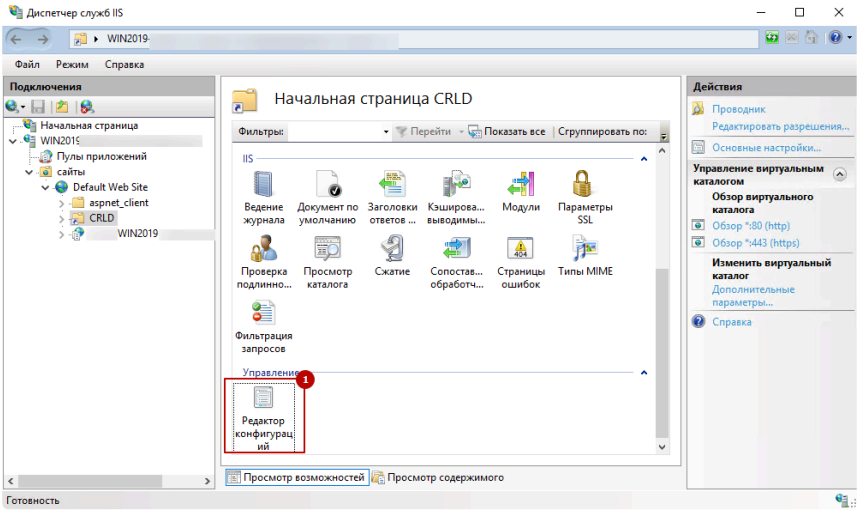


- В Диспетчере IIS выбрать **Имя сервера > Просмотр каталога > Включить**.

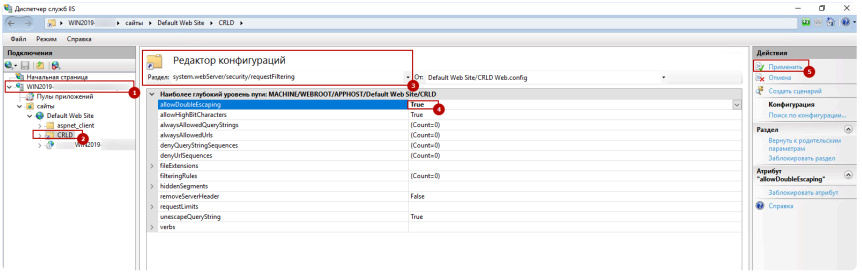




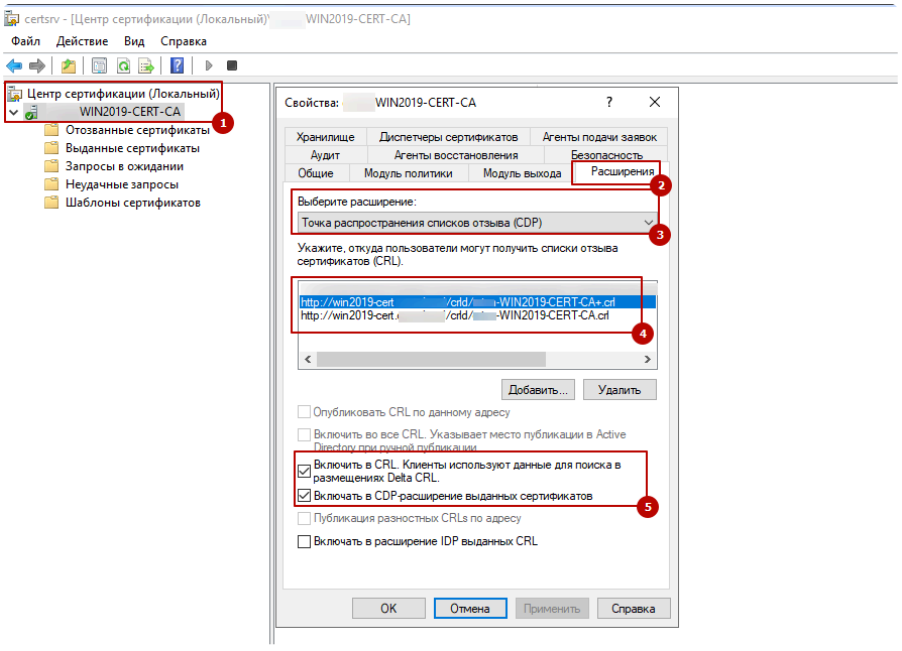
- В диспетчере IIS выбрать **Имя сервера > Сайты > Default Web Site > CRLD - Редактор конфигурации**.

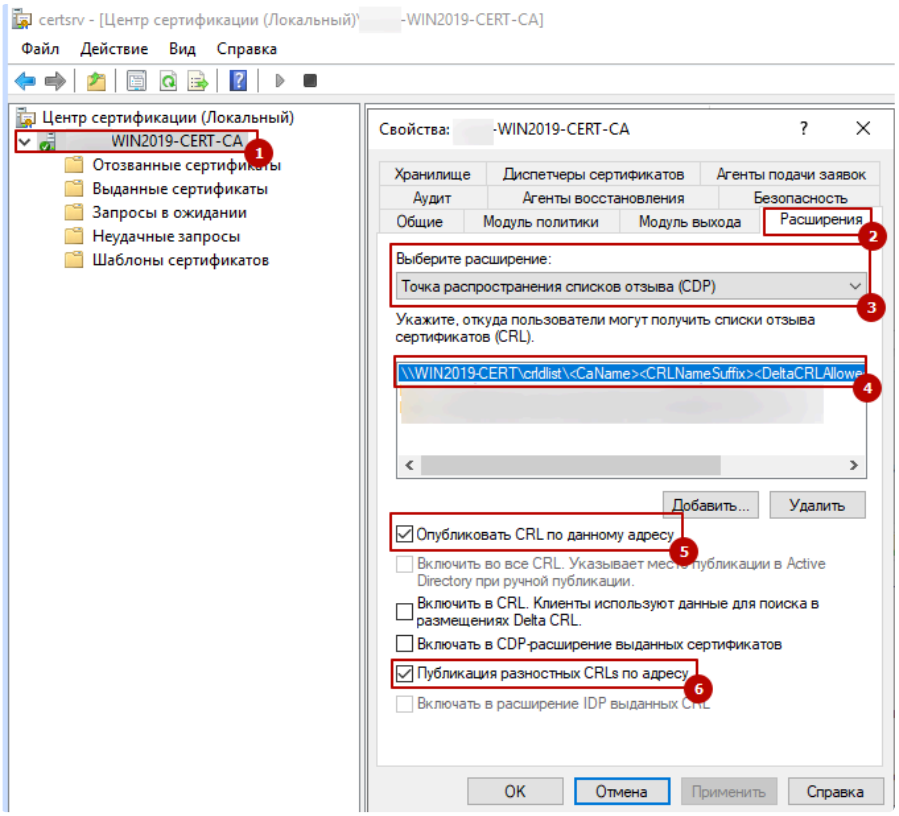


- В диспетчере IIS последовательно перейти в раздел **system.webServer/security/requestFiltering** и установить значение **allowDoubleEscaping > True > Применить**.



3. Произвести настройку CRL (списки SSL-сертификатов, отозванных центром выдачи). Для этого подключиться к консоли **Центр сертификации Windows > имя центра > ПКМ > Свойства > Расширения > Точка распространения списков отзыва CDP > Добавить** и добавить записи.
    - Запись 1: в поле **Размещение** указать:
        - http://<FQDN_имя_сервера>/crld/имя_центра_сертификации.crl (например http://win2019.mydomain.ru/crld/win2019-CA.crl).
        - Выбрать **Включить в CRL. Клиенты используют данные для поиска в размещения Delta CRL** и **Включать в CDP-расширение выданных сертификатов**.
    - Запись 2: в поле **Размещение** указать:
        - http://<FQDN_имя_сервера>/crld/имя_центра_сертификации.crl (например http://win2019.mydomain.ru/crld/win2019-CA+.crl).
        - Выбрать **Включить в CRL. Клиенты используют данные для поиска в размещения Delta CRL** и **Включать в CDP-расширение выданных сертификатов**.
    - Запись 3: в поле **Размещение** указать:
        - **\\<имя_сервера>\crldlist\<CaName><CRLNameSuffix><DeltaCRLAllowed.crl>** (например, **\\win2019\crldlist\<CaName><CRLNameSuffix><DeltaCRLAllowed.crl**).
        - Выбрать **Опубликовать CRL по данному адресу** и **Публикация разностных CRL по адресу**.





4. Опубликовать CRL.

   Для этого подключиться к консоли **Центр сертификации Windows > имя центра > Отозванные сертификаты > Все задачи > Публикация > Новый базовый CRL**. В папке **\\имя_сервера\crldlist** будут опубликованы 2 файла. Так же необходимо проверить, что при обращении в браузере к :

   - http://FQDN_имя_сервер/crld/имя_центра_сертификации.crl (например http://win2019.mydomain.ru/crld/win2019-CA.crl)
   - http://FQDN_имя_сервер/crld/имя_центра_сертификации+.crl (например http://win2019.mydomain.ru/crld/win2019-CA+.crl)

   происходит скачивание файла CRL.

5. Создать шаблон для выпуска сертификатов. Для этого подключиться к консоли **Центр сертификации Windows > имя центра > Шаблоны сертификатов > ПКМ > Управление**. Откроется консоль шаблона сертификатов. Для выпуска сертификата менеджера управления zVirt скопировать существующий шаблон **Веб сервер**. При копировании необходимо:

   - указать новое имя шаблона;
   - указать срок действия сертификата;
   - значения параметров режима совместимости выставить на **[Windows Server 2016]** в поле **Центр сертификации** и **[Windows 10 или Windows Server 2016]** в поле **Получатель сертификата**;
   - добавить разрешение на экспорт закрытого ключа;

- добавить тип шифрования
  [Microsoft Enhanced RSA and AES Cryptographic Provider];
- на вкладке **Безопасность** добавить полный доступ для **Компьютеры домена**, **Компьютер, с которого планируется выдача сертификатов**.

После подготовки шаблона необходимо закрыть **Консоль шаблона сертификатов.** В консоли **Центр сертификации > Шаблоны сертификатов** выбрать **Создать > Выдаваемый шаблон сертификата > имя шаблона, указанного на предыдущем шаге**. После этого, шаблон появится в списке центра сертификации. На основе этого шаблона можно получать сертификат через консоль MMC.

6. Выпустить сертификат для менеджера управления zVirt.

   Для этого открыть консоль MMC на сервере с установленной ролью **[Центр сертификации]** и последовательно выбрать **Файл > добавить или удалить оснастку > сертификаты > добавить > учётной записи компьютера > локальным компьютером**. Последовательно перейти **Сертификаты > Личное > сертификаты > все задачи > запросить новый сертификат > выбрать имя созданного шаблона > Требуется больше данных …**.

   Далее выбрать:

   - В поле "Полное имя DN": **CN=<имя_менеджера_управления_zVirt>**,**CN=<первая_часть_суффикса_доменного_имени>**,**CN=<вторая_часть_суффикса_доменного_имени>**.

     Например: **CN=zvirtmanager1,CN=company,CN=ru**
   - В поле "Общее имя": **<имя_менеджера_управления_zVirt>.<первая_часть_суффикса_доменного_имени>.<вторая_часть_суффикса_доменного_имени>**.

     Например **zvirtmanager1.company.ru**
   - В поле "Служба DNS": **<имя_менеджера_управления_zVirt>.<первая_часть_суффикса_доменного_имени>.<вторая_часть_суффикса_доменного_имени>**.

     Например **zvirtmanager1.company.ru**.
   - На вкладке **Общее** в поле **Понятное имя** указать имя, отображаемое в свойствах сертификата. Например **zvirtmanager1.company.ru**.

После выпуска сертификата экспортировать **2 сертификата**:

- Созданный на предыдущем шаге сертификат менеджера управления zVirt в формате **PFX**.

При экспорте указать: **[Да, экспортировать закрытый ключ]**, **[Экспортировать все расширенные свойства]**, **[Шифрование AES256-SHA256]**. Переименовать файл и его расширение в **apache.p12**. Обязательно убедиться, что p12 является расширением, а не частью названия - **apache.p12.pfx**.

- Корневой сертификат удостоверяющего центра в формате **CER**.

  При экспорте указать: **[Файлы X.509 (.CER) в кодировке BASE-64]**. Проверить корректной кодировки можно открыв данный сертификат блокнотом. Если кодировка корректна, то сертификат будет расположен между строками **-----BEGIN CERTIFICATE-----** и **-----END CERTIFICATE-----**. Переименовать файл и его расширение в **ca.cer**. Его можно экспортировать, открыв сертификат zVirt и перейдя на вкладку **[Путь сертификации]**. Нужно открыть корневой сертификат, перейти на вкладку **[Состав]** и нажать **[Копировать в файл]**.

Далее необходимо следовать инструкции.

Проверка срока истечения SSL сертификатов

Чтобы проверить сроки истечения сертификатов на хостах и менеджере управления нужно:

1. Скачать скрипт cert_date.sh.
2. Скопировать данный скрипт в удобное место на менеджере управления.
3. Дать скрипту права на выполнение командой.

```
chmod +x cert_date.sh
```

4. Выполнить скрипт

```
./cert_date.sh
```

Ошибка "device is rejected by filter config"

1. Описание ошибки

При работе с дисками может возникнуть ошибка:

```
Cannot use /dev/sdc1: device is rejected by filter config
```

2. Решение

Необходимо добавить устройство в фильтры lvm. Для этого произвести редактирование файла **/etc/lvm/lvm.conf**.

Было:

```
filter = ["a|^/dev/disk/by-id/lvm-pv-uuid-8Atbdn-U98I-gHsy-xDnc-d90s-jR8q-f2BCIj$|", "r|.*|"]
```

Стало:

```
filter = ["a|^/dev/disk/by-id/lvm-pv-uuid-8Atbdn-U98I-gHsy-xDnc-d90s-jR8q-f2BCIj$|", "a|/dev/sd*|", "r|.*|"]
```

Данное правило включает разрешающий фильтр для всех устройств **sda**, **sdb**, **sdc** и т.д.