Лабораторная работа №6

Работа ведется с использованием Oracle VM VirtualBox 4.2.6, Windows 2012 Server, Windows 8.

Задание: настроить и протестировать службу AD CS.

Настройка и проверка AD CS[1]

Шаг 1. Настройка компьютера ORCA1

Для настройки автономного корневого ЦС с именем ORCA1 необходимо выполнить следующие процедуры.

1. **Установка операционной системы.**
   - Не подключайте этот компьютер к сети.
   - Запустите установку Windows Server 2012.
   - Для завершения установки следуйте инструкциям, укажите Windows Server 2012 (полная установка) и надежный пароль для локальной учетной записи администратора. Войдите, используя локальную учетную запись администратора.
2. **Переименование компьютера.**
   - Откройте Windows PowerShell.
   - Введите команду rename-computer orca1 и нажмите клавишу ***ВВОД***.
   - Введите команду restart-computer и нажмите клавишу ***ВВОД***.
   - После перезапуска компьютера войдите под локальной учетной записью администратора.
3. **Подготовка файла CAPolicy.inf для автономного корневого ЦС.**
   - Откройте ***Windows PowerShell***, введите ***notepad c:\Windows\CAPolicy.inf*** и нажмите клавишу ***ВВОД***.
   - В ответ на запрос о создании нового файла нажмите кнопку ***Да***.
   - Введите в качестве содержимого файла следующее:

```
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
OID= 1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=http://www.contoso.com/pki/cps.txt
[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
CRLPeriod=weeks
CRLPeriodUnits=26
CRLDeltaPeriod=Days
CRLDeltaPeriodUnits=0
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=1
```

   - Нажмите кнопку ***Сохранить как***. Проконтролируйте следующие пункты: поле ***имя файла*** — CAPolicy.inf; ***тип файла*** — Все файлы; ***кодировка*** — ANSI.
4. **Установка автономного корневого ЦС.**
   - В окне диспетчера серверов щелкните ***Управление***, а затем нажмите кнопку ***Добавить роли и компоненты***.
   - На экране ***Приступая к работе*** нажмите кнопку ***Далее***.
   - Убедитесь, что на экране ***Выбор типа установки*** по умолчанию выбрано ***Установка ролей или компонентов***. Нажмите кнопку ***Далее***.

---

[1] http://technet.microsoft.com/ru-ru/library/hh831348

- На экране ***Выбор целевого сервера*** убедитесь, что выбран сервер ***orca1***, а затем нажмите кнопку ***Далее.***
- На экране ***Выбор ролей сервера*** выберите роль ***Службы сертификатов Active Directory***.
- При появлении предложения установить ***Средства удаленного администрирования сервера*** нажмите кнопку ***Добавить компоненты***. Нажмите кнопку ***Далее.***
- На экране ***Выбор компонентов*** нажмите кнопку ***Далее.***
- На экране ***Службы сертификатов Active Directory*** нажмите кнопку ***Далее.***
- На экране ***Выбор служб ролей*** по умолчанию выбрана роль ***Центр сертификации***. Нажмите кнопку ***Далее.***
- На экране ***Подтверждение выбранных элементов для установки*** проверьте информацию и нажмите кнопку ***Установить***.
- Дождитесь завершения установки. Во время установки двоичных файлов для ЦС отображается экран хода установки. После завершения установки двоичных файлов щелкните ссылку Настроить ***службы сертификатов Active Directory на конечном сервере.***
- На экране ***Учетные данные*** в поле ***Учетные данные*** должна отображаться строка ***ORCA1\Administrator***. Нажмите кнопку ***Далее.***
- На экране ***Службы ролей*** выберите ***Центр сертификации***. Это единственный доступный выбор, когда на сервере установлены только двоичные файлы для роли центра сертификации. Нажмите кнопку ***Далее.***
- На экране ***Вариант установки*** доступен единственный вариант: ***Автономный ЦС,*** так как учетная запись, использованная для установки, является членом локальной группы администраторов, а сервер не является членом домена доменных служб Active Directory (AD DS). Нажмите кнопку ***Далее.***
- На экране ***Тип ЦС*** по умолчанию выбрано ***Корневой ЦС***. Нажмите кнопку ***Далее.***
- На экране ***Закрытый ключ*** оставьте выбранный по умолчанию вариант ***Создать новый закрытый ключ***. Нажмите кнопку ***Далее.***
- Убедитесь, что на экране ***Шифрование для ЦС*** выбраны поставщик служб шифрования ***RSA#Microsoft Software Key Storage Provider***, длина ключа ***2048*** и хэш-алгоритм ***SHA1***, а затем нажмите кнопку ***Далее.***
- На экране ***Имя ЦС*** в текстовом поле ***Общее имя для этого ЦС*** введите ***ContosoRootCA***, а затем нажмите кнопку ***Далее.***
- На экране ***Срок действия*** введите ***20*** (число лет, в течение которых будет действителен сертификат).
- На экране ***База данных ЦС*** оставьте указанные по умолчанию расположения для базы данных и журнала базы данных. Нажмите кнопку ***Далее.***
- На экране ***Подтверждение*** нажмите кнопку ***Настроить***.
- В процессе настройки отображается экран ***Ход выполнения***, а по завершении операции — экран ***Результаты***. Нажмите кнопку ***Закрыть***. Если экран ***Ход установки*** все еще открыт, нажмите кнопку ***Закрыть*** и на этом экране.

5. **Настройка параметров корневого ЦС.**
   - В диспетчере серверов щелкните ***Сервис***, а затем выберите ***Центр сертификации***.
   - В дереве консоли центра сертификации разверните узел ***ORCA1-ContosoRootCA***. Щелкните правой кнопкой мыши элемент ***Отозванные сертификаты*** и выберите пункт ***Свойства***.
   - Убедитесь, что на вкладке ***Параметры публикации CRL*** не установлен флажок ***Включить публикацию разностных CRL***. Нажмите кнопку ***ОК.***
   - В дереве консоли центра сертификации щелкните правой кнопкой мыши объект ***ORCA1-ContosoRootCA*** и выберите пункт ***Свойства***.
   - Выберите вкладку ***Расширения***. Убедитесь, что в поле ***Выбор расширений*** установлен вариант ***Точка распространения списков отзыва (CDP)***, и просмотрите значения по умолчанию в разделе ***Выбор расположения, из которого пользователи могут получить список отзыва сертификатов (CRL)***.

- Измените значение ***Выбор расширения*** на ***Доступ к сведениям о центрах сертификации (AIA)*** и просмотрите значения по умолчанию. Нажмите кнопку ***ОК***. В диалоговом окне с приглашением перезапустить службы сертификатов ***Active Directory*** нажмите кнопку ***Нет***. Перезапуск службы будет выполнен после изменения путей по умолчанию на следующем этапе.
- В окне ***Windows PowerShell*** выполните следующие команды:

```
certutil -setreg CA\CRLPublicationURLs
"1:C:\Windows\system32\CertSrv\CertEnroll\%3%8.crl\n2:http://www.contoso.com/pki/%3%8.crl"

certutil –setreg CA\CACertPublicationURLs "2:http://www.contoso.com/pki/%1_%3%4.crt"

restart-service certsvc

certutil –crl
```

- Для просмотра AIA и CDP можно выполнить следующие команды: ***Get-CAAuthorityInformationAccess | format-list иGet-CACRLDistributionPoint | format-list***. Можно также вернуться на вкладку ***Расширения*** в диалоговом окне свойств центра сертификации и просмотреть, какие изменения были сделаны в AIA и CDP.

6. **Копирование сертификата корневого ЦС и списка отзыва сертификатов на съемный носитель.**
   - В ***Windows PowerShell*** выполните команду ***dir C:\Windows\system32\certsrv\certenroll*.cr****, которая отображает сертификаты и списки отзыва сертификатов (CRL) в хранилище сертификатов по умолчанию.
   - Скопируйте файл сертификата ЦС и список отзыва сертификатов на съемный носитель. Например, если вы выполняете команды для копирования сертификата и списка отзыва сертификатов на дисковод гибких дисков (A:), нужно будет выполнить следующие команды:
     - **copy C:\Windows\system32\certsrv\certenroll*.cr* A:**
     - **dir A:**
   - В приведенных выше командах укажите вместо ***A:*** букву, которой обозначен диск вашего съемного носителя. Съемный носитель может быть физическим или виртуальным. Если вы получите сообщение об ошибке ***"Не удалось распознать файловую систему тома"***, возможно, потребуется отформатировать носитель. Например, для гибкого диска, может быть, придется ввести команду ***format a:*** и нажать клавишу ***ВВОД***.
7. **Распространение корневого ЦС через объект групповой политики.**
   - Выполните вход на компьютер ***APP1*** с учетной записью ***"Пользователь1"***, которая является одновременно членом групп ***Domain Admins*** и ***Enterprise Admins***. Запустите программу ***Windows PowerShell*** от имени администратора. Для этого щелкните правой кнопкой мыши значок ***Windows PowerShell*** и выберите ***Запуск от имени администратора***. В открывшемся диалоговом окне ***"Контроль учетных записей"*** нажмите кнопку ***Да***.
   - Подключите съемный носитель, содержащий сертификат автономного корневого ЦС, к компьютеру ***APP1***.
   - В ***Windows PowerShell*** перейдите на съемный носитель при помощи команды ***cd*** (как при выполнении ***cd a:***\ для перехода в корневой каталог диска ***A***).
   - В окне ***Windows PowerShell*** на съемном диске выполните следующие команды:
     - **certutil –dspublish –f orca1_ContosoRootCA.crt RootCA**
     - **certutil –addstore –f root orca1_ContosoRootCA.crt**
     - **certutil –addstore –f root ContosoRootCA.crl**
   - *Первая команда помещает открытый сертификат корневого ЦС в контейнер конфигурации Active Directory. Это позволяет клиентским компьютерам домена автоматически доверять сертификату корневого ЦС, поэтому нет необходимости распределять этот сертификат в групповой политике. Вторая и третья команда помещают сертификат корневого ЦС и список отзыва сертификатов CRL в локальное хранилище компьютера APP1. В результате компьютер APP1 сразу становится доверенным благодаря открытому сертификату корневого ЦС и получает информацию о списке отзыва сертификатов корневого ЦС. Компьютер APP1 может получить сертификат из групповой политики, а список отзыва сертификатов (CRL) — из расположения CDP, но публикация этих двух объектов в локальном хранилище компьютера APP1 ускоряет настройку APP1 в качестве подчиненного ЦС.*

- *Открытые сертификаты, списки отзыва сертификатов и уведомление о правилах работы с сертификатами следует поместить в расположение http://www.contoso.com/pki. Внутренние клиентские компьютеры не смогут отображать имя этого компьютера на внутреннем веб-сайте (APP1), пока на DNS-сервере не появится соответствующая запись DNS.*

8. **Создание внутренней зоны DNS contoso.com и записи интернет-узла.**
   - На компьютере ***DC1*** откройте консоль ***DNS***. В диспетчере серверов щелкните ***Сервис***, а затем выберите ***DNS***.
   - В дереве консоли DNS разверните следующие элементы: ***DC1***, ***Зоны прямого просмотра***.
   - Щелкните правой кнопкой мыши ***Зоны прямого просмотра***, а затем выберите ***Новая зона***.
   - На экране мастера создания новой зоны нажмите кнопку ***Далее***.
   - По умолчанию выбрана ***Основная зона***, которая будет сохранена в ***Active Directory***. Чтобы использовать значения по умолчанию, нажмите кнопку ***Далее***.
   - Не изменяя значение по умолчанию, нажмите кнопку ***Далее***.
   - На экране ***Имя зоны*** введите ***contoso.com*** и нажмите кнопку ***Далее***.
   - На экране ***Динамическое обновление***, не изменяя заданные по умолчанию значения параметров, нажмите кнопку ***Далее***.
   - На экране ***Завершение мастера создания новой зоны*** нажмите кнопку ***Готово***.
   - В дереве консоли ***DNS*** щелкните правой кнопкой мыши зону ***contoso.com*** и выберите ***Новый узел*** (A или AAAA).
   - *Возможно, потребуется еще раз щелкнуть зону corp.contoso.com, чтобы открылся доступ к контекстному меню правой кнопки мыши.*
   - В поле ***Имя*** (если оставить пустым, будет использован родительский домен) введите ***www***.
   - В поле IP-адрес введите 10.0.0.3. Эта зона и запись будут направлять обращения внутренних клиентов к сайту ***www.contoso.com*** на адрес компьютера ***APP1***. Нажмите кнопку ***Добавить узел***.
   - Подтвердите создание записи, нажав кнопку ***ОК***. Нажмите кнопку ***Готово***.
   - Закройте консоль ***DNS***.

Шаг 2. Настройка компьютера APP1 для распределения сертификатов и списков отзыва сертификатов

В расширениях корневого ЦС было указано, что список отзыва сертификатов из корневого ЦС будет доступен по адресу ***http://www.contoso.com/pki***. В данный момент на компьютере ***APP1*** нет виртуального каталога ***PKI***, поэтому его необходимо создать. В рабочей среде обычно используют отдельные роли для выдающего ЦС и размещения ***AIA*** и ***CDP***. Однако в данной конфигурации лаборатории обе роли объединены, чтобы уменьшить количество ресурсов, необходимых для комплектации лаборатории.

Настройка компьютера APP1 для распределения сертификатов и списков отзыва сертификатов.

- Убедитесь, что вы вошли с учетной записью ***"Пользователь1"***. Запустите ***Windows PowerShell*** от имени администратора и выполните следующие команды.

```
New-item -path c:\pki –type directory
write-output "Example CPS statement" | out-file c:\pki\cps.txt
new-smbshare -name pki c:\pki "CORP\Domain Admins" -ChangeAccess "CORP\Cert Publishers"
```

- Откройте консоль ***IIS***. В диспетчере серверов щелкните ***Сервис*** и выберите ***Диспетчер Internet Information Services (IIS)***.
- В дереве консоли диспетчера ***Internet Information Services (IIS)*** разверните узел компьютера ***APP1***. Если появится приглашение приступить к работе с веб-платформой Майкрософт, нажмите кнопку ***Отмена***.
- Разверните ***Сайты***, щелкните правой кнопкой мыши ***Default Web Site*** и выберите ***Добавить виртуальный каталог***.

- В поле ***Псевдоним*** введите ***pki***, в поле ***"Физический путь"*** введите ***C:\pki***, а затем нажмите кнопку ***ОК***.
- Разрешите анонимный доступ к виртуальному каталогу ***pki***. Для этого выполните следующие действия.
  - Убедитесь, что на панели ***Подключения*** выбрано ***pki***.
  - На домашней странице ***pki*** щелкните ***Проверка подлинности***.
  - На панели ***Действия*** щелкните ***Изменение разрешений***.
  - На вкладке ***Безопасность*** щелкните ***Изменить***.
  - В диалоговом окне ***Разрешения для pki*** нажмите кнопку ***Добавить***.
  - В диалоговом окне ***Выбор пользователей, компьютеров, учетных записей служб или групп*** введите ***Издатели сертификатов***, затем нажмите кнопку ***Проверить имена***.
  - В диалоговом окне ***Выбор пользователей, компьютеров, учетных записей служб или групп*** нажмите кнопку ***Типы объектов***.
  - В диалоговом окне ***Типы объектов*** выберите ***Учетные записи служб*** и нажмите кнопку ***ОК***.
  - В диалоговом окне ***Выбор пользователей, компьютеров, учетных записей служб или групп*** нажмите кнопку ***Размещение***.
  - В диалоговом окне ***Размещение*** выберите компьютер ***APP1*** и нажмите кнопку ***ОК***.
  - В диалоговом окне ***Выбор пользователей, компьютеров, учетных записей служб или групп*** после ***Издатели сертификатов*** введите ***;IIS AppPool\DefaultAppPool***, а затем нажмите кнопку ***Проверить имена***. Нажмите кнопку ***ОК***.
- *В результате описанных действий пулу приложений IIS по умолчанию предоставляются следующие разрешения: Чтение и выполнение, Вывод списка содержимого папки и Чтение. IIS использует пул приложений по умолчанию, чтобы разрешить анонимный доступ. Благодаря этому пользователям разрешается проверять AIA и CDP, размещенные на IIS.*
  - В диалоговом окне ***Разрешения для pki*** выберите ***Издатели сертификатов*** (CORP\Издатели сертификатов). В диалоговом окне ***Разрешения для издателей сертификатов*** установите флажок ***Изменить*** в столбце ***Разрешить*** и дважды нажмите кнопку ***ОК***.
- *Предоставление измененных разрешений для папки pki Cert Publishers позволяет ЦС в организации публиковать сертификаты и списки отзыва сертификатов (CRL) в этой папке.*
- На панели ***Домашняя страница pki*** дважды щелкните ***Фильтрация запросов***.
- Вкладка ***Расширения имен файлов*** на панели ***Фильтрация запросов*** выбрана по умолчанию. На панели ***Действия*** щелкните ***Изменение параметров функций***.
- В диалоговом окне ***Изменение параметров фильтрации запросов*** выберите ***Разрешить двойное преобразование символов*** и нажмите кнопку ***ОК***. Закройте диспетчер ***Internet Information Services (IIS)***.
- Запустите ***Windows PowerShell*** от имени администратора. В окне ***Windows PowerShell*** выполните команду ***iisreset***.

Шаг 3. Настройка компьютера APP1 в качестве подчиненного ЦС предприятия

Для настройки APP1 в качестве подчиненного ЦС предприятия необходимо выполнить следующие действия:

1. **Конфигурация файла CAPolicy.inf.**
   - На компьютере ***APP1***, выполнив вход с учетной записью ***"Пользователь1"***, откройте программу ***Windows PowerShell*** от имени администратора, а затем введите ***notepad c:\Windows\CAPolicy.inf*** и нажмите ***ВВОД***.
   - При появлении запроса, хотите ли вы создать файл, нажмите кнопку ***Да***.
   - Используйте для файла подчиненного ЦС предприятия ***CAPolicy.inf*** следующую информацию.

```
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
```

```
Policies=InternalPolicy
[InternalPolicy]
OID= 1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=http://www.contoso.com/pki/cps.txt
[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=1
```

- Выберите команду меню ***Файл, Сохранить как*** и убедитесь, что для сохраняемого файла указана кодировка ***ANSI***, имя ***CAPolicy.inf*** и папка ***C:\Windows***. Чтобы можно было указать расширение ***.inf*** вместо расширения ***.txt***, выберите в поле Тип файла — ***Все файлы***. Когда появится запрос на замену файла ***CAPolicy.inf***, нажмите кнопку ***Да***.
- Закройте ***Блокнот***.

2. Установка роли подчиненного ЦС предприятия.

- На компьютере ***APP1*** под учетной записью ***"Пользователь1"*** запустите ***Windows PowerShell*** от имени администратора, а затем выполните следующую команду: ***gpupdate /force***. Это действие обеспечивает применение на компьютере ***APP1*** объекта групповой политики для доверенного корневого ЦС.
- В окне диспетчера серверов щелкните ***Управление***, а затем нажмите кнопку ***Добавить роли и компоненты***.
- На экране ***Прежде чем приступить к работе*** нажмите кнопку ***Далее***.
- Убедитесь, что на экране ***Выбор типа установки*** по умолчанию выбрано ***Установка ролей и компонентов***. Нажмите кнопку ***Далее***.
- На экране ***Выбор целевого сервера*** убедитесь в том, что выбран сервер ***APP1***, а затем нажмите кнопку ***Далее***.
- На экране ***Выбор ролей сервера*** выберите роль ***Службы сертификатов Active Directory***.
- На экране с предложением установить С***редства удаленного администрирования сервера*** нажмите кнопку ***Добавить компоненты***. Нажмите кнопку ***Далее***.
- На экране ***Выбор компонентов*** нажмите кнопку ***Далее***.
- На экране ***Службы сертификатов Active Directory*** нажмите кнопку ***Далее***.
- На экране ***Выбор служб ролей*** убедитесь, что выбрана роль ***Центр сертификации***, а затем нажмите кнопку ***Далее***.
- На экране ***Подтверждение выбранных элементов для установки*** проверьте информацию и нажмите кнопку ***Установить***.
- Дождитесь завершения установки. Во время установки двоичных файлов для ЦС отображается экран хода установки. После завершения установки двоичных файлов щелкните ссылку ***Настроить службы сертификатов Active Directory на конечном сервере***.
- На экране ***Учетные данные*** отображаются учетные данные для учетной записи ***"Пользователь1"***. Нажмите кнопку ***Далее***.
- На экране ***Службы ролей*** выберите ***Центр сертификации***.
- На экране ***Вариант установки*** убедитесь, что выбран параметр ЦС предприятия, и нажмите кнопку ***Далее***.
- На экране ***Тип ЦС*** выберите тип ***Подчиненный ЦС*** для установки подчиненного ЦС предприятия. Нажмите кнопку ***Далее***.
- Убедитесь, что на экране ***Закрытый ключ*** выбрано значение ***Создать новый закрытый ключ***, и нажмите кнопку ***Далее***.
- На экране ***Шифрование для ЦС*** должны быть указаны следующие сведения: поставщик служб шифрования — ***Поставщик хранилища ключей RSA#Microsoft Software***, длина ключа — ***2048*** и хэш-алгоритм — ***SHA1***. Нажмите кнопку ***Далее***.
- На экране ***Имя ЦС*** в поле ***Общее имя для этого ЦС*** введите ***IssuingCA-APP1***. Различающееся имя изменится на ***CN=IssuingCA-APP1,DC=corp,DC=contoso,DC=com***. Нажмите кнопку ***Далее***.
- Обратите внимание, что на экране ***Запрос сертификата*** выбран параметр ***Сохранить запрос сертификата в файле на конечном компьютере***. Это правильная настройка

параметра, так как в данной конфигурации мы используем автономный родительский ЦС (корневой ЦС). Не изменяя значения по умолчанию, нажмите кнопку ***Далее***.

- На экране ***База данных ЦС***, не изменяя заданные по умолчанию значения, нажмите кнопку ***Далее***.
- На экране ***Подтверждение*** нажмите кнопку ***Настроить***.
- На экране ***Результаты*** появится уведомление о том, что для завершения настройки необходимо отправить запрос сертификата в ЦС ***ContosoRootCA***. Нажмите кнопку ***Закрыть***.
- Скопируйте запрос сертификата на съемный носитель и перенесите его на компьютер ***ORCA1***. Например, если нужно скопировать файл с диска ***C:*** на гибкий диск ***A:***, можно выполнить следующую команду из ***Windows PowerShell***: ***copy C:*.req A:***
- Подключите съемный носитель с файлом запроса сертификата к компьютеру ***ORCA1***. Выполните вход в корневой ЦС с учетной записью, которая является членом локальной группы ***Administrators***.
- На компьютере ***ORCA1*** из ***Windows PowerShell*** отправьте запрос при помощи следующей команды (при условии, что буква вашего съемного носителя ***A:***):
  certreq -submit A:\APP1.corp.contoso.com_IssuingCA-APP1.req
- Убедитесь, что в поле ***Список центров сертификации*** выбран ЦС ***ContosoRootCA (Kerberos)***, и нажмите кнопку ***ОК***. На экране появится идентификационный номер запроса и сообщение о том, что запрос ожидает выполнения. Обязательно сохраните идентификационный номер запроса.
- На компьютере ***ORCA1*** в диспетчере серверов выберите ***Сервис***, а затем ***Центр сертификации***. Разверните объект ***ContosoRootCA*** и выберите ***Запросы в ожидании***.
- Правой кнопкой мыши щелкните идентификационный номер запроса, совпадающий с номером, который вы видели, когда отправляли запрос на предыдущем этапе. Выберите ***Все задачи***, затем ***Выдать***.
- Щелкните ***Выданные сертификаты*** и просмотрите выданный сертификат на панели ***Сведения***.
- На компьютере ***ORCA1*** вернитесь в командную строку и получите выданный сертификат при помощи команды
  certreq –retrieve <Идентификатор_запроса> <диск>:\APP1.corp.contoso.com_corp-APP1-CA.crt.
  Вместо ***<Идентификатор_запроса>*** укажите реальный номер переданного запроса, а вместо ***<диск>*** — реальную букву съемного носителя. Например, если идентификационный номер запроса 2, а буква съемного носителя A, получится следующая команда: certreq –retrieve 2 a:\APP1.corp.contoso.com_IssuingCA-APP1.crt. В диалоговом окне для выбора центра сертификации убедитесь, что выбран ***ORCA1-ContosoRootCA***, и нажмите кнопку ***ОК***.
- На компьютере ***ORCA1*** выполните команду ***dir A:*** (если буква съемного носителя A; в противном случае замените букву A). На съемном носителе будут сохранены файлы ***ContosoRootCA.crl***, ***orca1_ORCA1-ContosoRootCA.crt*** и ***APP1.corp.contoso.com_corp-APP1-CA.crt***. Подключите съемный носитель к компьютеру ***APP1***.
- На компьютере ***APP1*** в ***Windows PowerShell*** скопируйте сертификаты и списки отзыва сертификатов (***CRL***) в папку ***pki*** при помощи следующих команд (при условии, что A: соответствует букве съемного носителя; в противном случае укажите правильную букву диска):
  copy a:*.cr* c:\pki
- На компьютере ***APP1*** в консоли ***Центра сертификации*** щелкните правой кнопкой мыши объект ***IssuingCA-APP1*** и выберите ***Все задачи***, а затем ***Установить сертификат ЦС***.
- В диалоговом окне ***Выберите файл для завершения установки ЦС*** выберите тип файла ***Сертификат X.509*** (*.cer; *.crt), перейдите к съемному носителю и выберите файл ***APP1.corp.contoso.com_IssuingCA-APP1.crt***. Нажмите кнопку ***Открыть***.
- Запустите службы сертификации ***Active Directory***. Для этого щелкните правой кнопкой мыши объект ***corp-APP1-CA*** и выберите ***Все задачи***, а затем ***Запустить службу***.

- На компьютере ***APP1*** скопируйте список отзыва сертификатов с компьютера в папку ***C:\pki***. В окне ***Windows PowerShell*** выполните команду copy ***c:\Windows\system32\certsrv\certenroll*.cr* c:\pki***

3. **Настройка AIA и CDP.**
   - На компьютере ***APP1*** с учетной записью ***"Пользователь1"*** щелкните правой кнопкой ***Windows PowerShell*** и выберите ***Запуск от имени администратора***. Нажмите кнопку ***Да***, чтобы подтвердить, что вы хотите выполнить ***Windows PowerShell*** от имени администратора.
   - В окне ***Windows PowerShell*** выполните следующие команды:

```
certutil -setreg CA\CRLPublicationURLs
"65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n6:http://www.contoso.com/pki/%3%8%9.crl\n65:file://\
\App1.corp.contoso.com\pki\%3%8%9.crl"

certutil -setreg CA\CACertPublicationURLs "2:http://www.contoso.com/pki/%1_%3%4.crt"
```

   - Чтобы перезапустить службу ЦС, в окне ***Windows PowerShell*** выполните следующие команды: ***restart-service certsvc***
   - Для публикации списка отзыва сертификатов в окне ***Windows PowerShell*** выполните следующую команду: ***certutil –crl***

Шаг 4. Настройка автоматической регистрации сертификатов компьютера

Для настройки автоматической регистрации сертификатов компьютера необходимо выполнить две процедуры.

1. **Включение автоматической регистрации сертификатов через групповую политику.**
   - На компьютере ***DC1*** войдите в систему с учетной записью ***"Пользователь1"***. В диспетчере серверов выберите ***Сервис***, а затем ***Управление групповой политикой***.
   - В дереве консоли разверните следующие объекты: ***Лес corp.contoso.com***, ***Домены***, ***corp.contoso.com***.
   - В дереве консоли щелкните правой кнопкой мыши объект ***Политика домена по умолчанию***, а затем выберите команду ***Изменить***.
   - В дереве консоли редактора управления групповыми политиками в категории ***Конфигурация компьютера*** разверните следующие объекты: ***Политики***, ***Параметры Windows***, ***Параметры безопасности***, а затем выберите ***Политики открытого ключа***.
   - На панели подробностей дважды щелкните параметр ***Клиент службы сертификации: автоматическая регистрация***. В окне ***Модель конфигурации*** выберите параметр ***Включено***.
   - Установите флажки ***Обновлять сертификаты с истекшим сроком действия или в состоянии ожидания и удалять отозванные сертификаты*** и ***Обновлять сертификаты, использующие шаблоны сертификатов***. Нажмите кнопку ***ОК***.
   - Закройте редактор управления групповыми политиками и консоль управления групповыми политиками.
2. **Определение шаблона сертификата проверки подлинности клиента и сервера для автоматической регистрации.**
   - На компьютере ***APP1*** на панели консоли центра сертификации убедитесь, что объект ***IssuingCA-APP1*** развернут.
   - Щелкните правой кнопкой мыши элемент ***Шаблоны сертификатов*** и выберите команду ***Управление***.
   - На панели подробностей щелкните правой кнопкой мыши ***Проверка подлинности рабочей станции***, а затем выберите команду ***Скопировать шаблон***.
   - Перейдите на вкладку ***Общие*** и в поле ***Отображаемое имя шаблона*** введите ***Client-Server Authentication***.
   - Перейдите на вкладку ***Расширения***, убедитесь, что выбраны ***Политики применения***, и нажмите кнопку ***Изменить***.
   - Нажмите кнопку ***Добавить***, затем щелкните ***Проверка подлинности сервера***. Дважды нажмите кнопку ***ОК***.
   - В диалоговом окне ***Свойства нового шаблона*** перейдите на вкладку ***Безопасность***.

- В окне ***Группы или пользователи*** нажмите кнопку ***Компьютеры домена (CORP\Компьютеры домена)***.
- В строке ***Автоматическая подача заявок*** установите флажок ***Разрешить***. В результате этого действия все компьютеры домена будут автоматически запрашивать сертификаты с помощью данного шаблона.
- Нажмите кнопку ***ОК***. Закройте ***Консоль шаблонов сертификатов***.
- Щелкните правой кнопкой мыши контейнер ***Шаблоны сертификатов***, выберите команду ***Создать***, а затем — пункт ***Выдаваемый шаблон сертификата***.
- В диалоговом окне ***Включение шаблонов сертификатов*** щелкните ***Client-Server Authentication*** и нажмите кнопку ***ОК***. Закройте консоль центра сертификации.

Шаг 5. Настройка протокола SSL для компьютера APP1

Чтобы продемонстрировать, как могут использоваться сертификаты, развернутые через доменные службы ***Active Directory*** и службы сертификации ***Active Directory***, обеспечьте защиту веб-сайта ***APP1*** при помощи протокола ***SSL*** и подключите компьютер ***CLIENT1*** к этому защищенному сайту.

Эта часть выполняется, чтобы продемонстрировать защиту веб-сайта с помощью сертификата.

Данный шаг включает две процедуры.

1. **Обеспечение защиты веб-сайта APP1 по умолчанию.**
   - На компьютере ***APP1*** с учетной записью ***"Пользователь1"*** запустите ***Windows PowerShell*** от имени администратора. Затем выполните следующие команды:
     Gpupdate /force. Подождите, пока завершится обновление групповой политики, после этого закройте командную строку. При этом компьютеру APP1 автоматически будет выдан сертификат, распространенный с помощью групповой политики.
     ```
     cd cert:\LocalMachine\My
     dir | format-list
     ```
   - Вы увидите, что у вас имеется два сертификата. Один из них выдан ***ContosoRootCA***, это сертификат ЦС компьютера ***APP1***. Второй сертификат был выдан ***IssuingCA-APP1*** и может быть использован для обеспечения безопасности веб-сайта по умолчанию на ***APP1***.
   - Откройте консоль диспетчера ***Internet Information Services (IIS)***. В диспетчере серверов щелкните ***Сервис*** и выберите ***Диспетчер Internet Information Services (IIS)***. На панели содержимого разверните следующий путь: ***APP1, Сайты, Default Web Site***.
   - Выберите объект ***Default Web Site***. На панели ***Действия*** щелкните элемент ***Привязки***.
   - В диалоговом окне ***Привязки сайта*** нажмите кнопку ***Добавить***.
   - В диалоговом окне ***Добавление привязки сайта*** выберите в списке ***Тип*** значение ***https***.
   - В разделе ***Сертификат SSL*** нажмите кнопку ***Выбор***.
   - В разделе ***Выбор сертификата*** в поле выбора выберите сертификат, выданный ЦС ***IssuingCA-APP1*** через групповую политику. Это будет сертификат с длинным буквенно-цифровым значением, в отличие от сертификата ***IssuingCA-APP1***. Чтобы убедиться в правильном выборе сертификата, нажмите кнопку ***Просмотреть***. Убедитесь, чтобы в выбранном сертификате было написано, что он выдан ***APP1.corp.contoso.com*** центром сертификатов ***IssuingCA-APP1***. Убедившись в правильности сертификата, нажмите кнопку ***ОК*** в диалоговом окне ***Сертификат***.
   - В диалоговом окне ***Добавление привязки сайта*** нажмите кнопку ***ОК***.
   - В диалоговом окне ***Привязки сайта*** нажмите кнопку ***Закрыть***.
2. **Подключение к защищенному веб-сайту.**
   - Подключите компьютер ***CLIENT1*** к корпоративной сети.
   - Войдите в систему компьютера ***CLIENT1*** под учетной записью ***Пользователя1***.
   - Откройте на компьютере ***CLIENT1 Internet Explorer***.
   - В адресной строке ***Internet Explorer*** введите адрес ***https://app1.corp.contoso.com*** и нажмите ***ВВОД***. Открывшаяся веб-страница ***IIS 8***, используемая по умолчанию, подтверждает, что привязки ***https*** и ***SSL*** для веб-сайта по умолчанию на компьютере ***APP1*** работают.