

Установка центра сертификации на предприятии.

Часть 3 / Хабр

 habr.com/ru/companies/microsoft/articles/349202

Alexander Gureev

March 1, 2018



А вот и финальная третья часть нашей серии статей о центре сертификации на предприятии. Сегодня рассмотрим развертывание службы сертификатов на примере Windows Server 2016. Поговорим о подготовке контроллера домена, подготовке веб-сервера, установке корневого и издающего центров сертификации и об обновлении сертификатов. Заглядывайте под кат!

Словарь терминов

В этой части серии использованы следующие сокращения и аббревиатуры:

- **PKI** (*Public Key Infrastructure*) — инфраструктура открытого ключа, набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей. Поскольку аббревиатура ИОК не является распространённой, здесь и далее будет использоваться более знакомая англоязычная аббревиатура PKI.
- **X.509** — стандарт [ITU-T](#) для инфраструктуры открытого ключа и инфраструктуры управления привилегиями.
- **ЦС** (*Центр Сертификации*) — служба выпускающая цифровые сертификаты. Сертификат — это электронный документ, подтверждающий принадлежность открытого ключа владельцу.
- **CRL** (*Certificate Revocation List*) — список отзыва сертификатов. Подписанный электронный документ, публикуемый ЦС и содержащий список отозванных сертификатов, действие которых прекращено по внешним причинам. Для каждого отозванного сертификата указывается его серийный номер, дата и время отзыва, а также причина отзыва (необязательно). Приложения могут использовать CRL для подтверждения того, что предъявленный сертификат является действительным и не отозван издателем... Приложения могут использовать CRL для подтверждения, что предъявленный сертификат является действительным и не отозван издателем.

- **SSL** (*Secure Sockets Layer*) или **TLS** (*Transport Layer Security*) — технология обеспечивающая безопасность передачи данных между клиентом и сервером поверх открытых сетей.
- **HTTPS** (*HTTP/Secure*) — защищённый HTTP, является частным случаем использования SSL.
- **Internet PKI** — набор стандартов, соглашений, процедур и практик, которые обеспечивают единый (унифицированный) механизм защиты передачи данных на основе стандарта X.509 по открытым каналам передачи данных.
- **CPS** (*Certificate Practice Statement*) — документ, описывающий процедуры управления инфраструктурой открытого ключа и цифровыми сертификатами.

Общий план развёртывания

Для развёртывания службы сертификатов нам потребуется четыре машины с Windows Server 2016, которые будут выполнять следующие функции:

1. **Контроллер домена** — необходим для функционирования домена Active Directory;
2. **Веб-сервер** — будет обеспечивать доступ к сертификатам ЦС и спискам отзывов для клиентов;
3. **Корневой ЦС** — будет выполнять функции корневого ЦС;
4. **Подчинённый ЦС** — будет выполнять функции издающего ЦС.

Развёртывание PKI будет проходить поэтапно на каждом сервере в том порядке, в котором они указаны выше. Подготовка контроллера домена будет сводиться к обеспечению функций Active Directory, GPO и учётных записей.

Подготовка контроллера домена

Перед развёртыванием PKI необходимо убедиться в работоспособности домена Active Directory и что все необходимые серверы (а именно, веб-сервер и подчинённый ЦС) введены в домен. А так же, что подготовлены необходимые учётные записи. На данном этапе нам потребуется только учётная запись с правами Enterprise Admins.

Ряд операций на подчинённом ЦС требуют прав Enterprise Admins, поскольку производится запись в раздел configuration naming context. Если это корневой домен леса, то для этих операций достаточно прав Domain Admins.

Следующим шагом будет конфигурирование политики автоматической выдачи сертификатов (autoenrollment). Эта политика нужна будет в процессе эксплуатации

служб сертификатов для автоматической выдачи и обновления истёкших сертификатов на клиентах. Политика настраивается в конфигурации компьютера и пользователя:

- Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Infrastructure\Certificate Services Client – Auto-Enrollment
- User Configuration\Policies\Windows Settings\Security Settings\Public Key Infrastructure\Certificate Services Client – Auto-Enrollment

Политика в обоих разделах должна быть сконфигурирована как показано на следующей картинке:

Certificate Services Client - Auto-Enrollment Properties ? X

Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

☒ Renew expired certificates, update pending certificates, and remove revoked certificates

☒ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

Additional stores. Use ", " to separate multiple stores. For example:
"Store 1, Store 2, Store 3"

OK Cancel Apply

Сконфигурированный объект групповых политик (GPO) должен быть пристыкован к корню домена. Данную процедуру необходимо повторить во всех доменах текущего леса Active Directory. Далее, необходимо создать запись типа CNAME с именем CDP на сервере ДНС, который будет указывать на веб-сервер (IIS). Эту процедуру необходимо выполнить как на внутреннем, так и на внешнем (который обслуживает зону в интернете) серверах ДНС. Запись можно создать при помощи PowerShell:

```
Add-DnsServerResourceRecord -CName -Name "cdp" -HostNameAlias "iis.contoso.com" -ZoneName "contoso.com"
```

Подготовка веб-сервера

На веб-сервере нам потребуется выполнить следующее: установить службу IIS (если ещё не установлена), создать общую папку и сконфигурировать веб-сайт на использование этой папки.

Установка службы IIS

Для установки службы IIS можно воспользоваться следующей командой:

```
Install-WindowsFeature -Name Web-Server, Web-WebServer -IncludeManagementTools
```

Создание папки PKIdata

Согласно нашей конфигурационной таблице (см. часть 2), для хранения сертификатов ЦС и списков отзыва нам потребуется общая папка с сетевым именем PKI по следующему пути: C:\InetPub\wwwroot\PKIdata

```
New-Item -ItemType Directory -Path C:\InetPub\wwwroot -Name PKIdata -Force  
New-SmbShare -Path C:\inetpub\wwwroot\PKIdata -Name PKI -FullAccess everyone
```

После этого нужно выдать права NTFS на запись в эту папку для группы Cert Publishers.

Создание веб-сайта

Теперь нам необходимо создать отдельный веб-сайт с именем “CDP” и хост-именем “cdp.contoso.com”:

```
New-Website -Name CDP -HostHeader cdp.contoso.com -PhysicalPath  
C:\inetpub\wwwroot\PKIdata  
New-WebVirtualDirectory -Site cdp -Name pki -PhysicalPath  
C:\inetpub\wwwroot\PKIdata
```

Включение поддержки Delta CRL

В нашем сценарии издающий ЦС будет публиковать Delta CRL, которые содержат символ плюс «+» в имени файла (например, contoso-pica+.crl). По умолчанию, IIS будет расценивать этот символ в запросе как метасимвол и не позволит клиентам скачать список отзыва. Для этого необходимо включить двойной эскейпинг в настройках IIS, чтобы расценивать знак плюса в запросе как литерал:

```
Import-Module -Name WebAdministration
Set-WebConfigurationProperty -PSPath 'MACHINE/WEBROOT/APPHOST' -Filter
/system.webServer/security/requestFiltering -name allowdoubleescaping -Value
'true'
```

Установка корневого ЦС

Фактическая установка ЦС будет включать в себя несколько этапов:

1. Подготовка предустановочных конфигурационных файлов (CAPolicy.inf);
2. Установка компонента ЦС;
3. Выполнение постустановочной конфигурации;
4. Проверка установки.

Перед установкой корневого ЦС, необходимо ещё раз вернуться к конфигурационным таблицам:

Название параметра	Значение параметра
Сервер ЦС	
Класс ЦС	Standalone CA
Тип ЦС	Root CA
Сертификат	
Имя сертификата	Contoso Lab Root Certification authority
Дополнительный суффикс	OU=Division Of IT, O=Contoso Pharmaceuticals, C=US
Провайдер ключа	RSA#Microsoft Software Key Storage Provider
Длина ключа	4096 бит
Алгоритм подписи	SHA256
Срок действия	15 лет

В таблице я выделил только те параметры, которые задаются до и в процессе установки. Остальные параметры будут настраиваться после установки.

Предварительная конфигурация

Предварительные конфигурационные файлы необходимы для ряда настроек, которые невозможно задать во время установки компонента (ни при помощи графического интерфейса, ни при помощи командной строки или PowerShell). К ним

обычно относятся настройки расширений сертификата ЦС. Например, для настройки расширения сертификата Certificate Policies, необходимо использовать предварительный конфигурационный файл, в котором настраиваются параметры расширения. Для Microsoft AD CS таким файлом является файл CAPolicy.inf, который должен быть расположен по следующему пути: %windir%\CAPolicy.inf. С синтаксисом этого файла можно ознакомиться в следующей статье: [How CA Certificates Work](#). Поскольку никаких специфичных или нестандартных настроек в сертификате корневого ЦС мы делать не будем, поэтому и предварительный конфигурационный файл сейчас нам не потребуется.

Установка компонента ЦС

Прежде всего необходимо добавить установочные компоненты для AD CS:

```
Install-WindowsFeature -Certificate, ADCS-Cert-Authority -IncludeManagementTools
```

После этого сверьтесь с предыдущей таблицей, чтобы определить параметры установки. Исходя из данных таблицы, зададим параметры для командлета [Install-AdcsCertificationAuthority](#):

```
Install-AdcsCertificationAuthority -CACommonName "Contoso Lab Root Certification Authority" `
  -CADistinguishedNameSuffix "OU=Division Of IT, O=Contoso Pharmaceuticals, C=US" `
  -CAType StandaloneRootCA `
  -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
  -KeyLength 4096 `
  -HashAlgorithmName SHA256 `
  -ValidityPeriod "years" `
  -ValidityPeriodUnits 15 `
  -DatabaseDirectory $(Join-Path $env:SystemRoot "System32\CertLog")
```

Итоговая настройка

После установки компонента ЦС необходимо настроить рабочие параметры ЦС. Рассмотрим ещё раз элементы, которые нам необходимо настроить:

Название параметра	Значение параметра
Сервер ЦС	
Срок действия издаваемых сертификатов	15 лет

Точки публикации CRT	1) По-умолчанию 2) C:\CertData\contoso-rca<CertificateName>.crt 3) IIS:\inetPub\PKIdata\contoso-rca<CertificateName>.crt*
Точки распространения CRT	1) <a href="http://cdp.contoso.com/pki/contoso-rca<CertificateName>.crt">cdp.contoso.com/pki/contoso-rca<CertificateName>.crt
Точки публикации CRL	1) По-умолчанию 2) C:\CertData\contoso-rca<CRLNameSuffix>.crt 3) IIS:\inetPub\PKIdata\contoso-rca<CRLNameSuffix>.crt*
Точки распространения CRL	1) <a href="http://cdp.contoso.com/pki/contoso-rca<CRLNameSuffix>.crt">cdp.contoso.com/pki/contoso-rca<CRLNameSuffix>.crt

Сертификат

Состав CRL	Base CRL
	Base CRL
Тип	Base CRL
Срок действия	6 месяцев
Расширение срока действия	1 месяц
Алгоритм подписи	SHA256
Публикация в AD	Нет

* — копируется на сервер IIS

Скрипт настройки

Для конфигурирования настроек ЦС мы будем использовать BATCH скрипт с использованием утилиты certutil.exe:


```

:.....
:
::
::
:.....
:
:: все комментарии помечены знаком двойного двоеточия (::)
:: записываем пути для публикации и распространения сертификатов ЦС и списков
отзыва
:: в отдельные переменные
SET CrlLocal=C:\CertData\contoso-rca%%8.crl
SET CDP=http://cdp.contoso.com/pki/contoso-rca%%8.crl
SET AIA=http://cdp.contoso.com/pki/contoso-rca%%4.crt :: Создаём папку в корне
системного диска, куда будут записываться файлы ЦС. Эта папка
:: создаётся для удобства, чтобы не искать папку CertEnroll в глубине папки
Windows.
md C:\CertData :: Настраиваем пути публикации и распространения для сертификатов
ЦС и списков отзыва.
certutil -setreg CA\CRLPublicationURLs
"1:%windir%\system32\CertSrv\CertEnroll\%%3%%8.crl\n1:%CrlLocal%\n2:%CDP%" certuti
l -setreg CA\CACertPublicationURLs
"1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:%AIA%" :: Поскольку мы
не можем указывать пути публикации для файла сертификата, мы
:: вручную переименовываем его в необходимый формат и копируем в папку CertData
ren %windir%\system32\CertSrv\CertEnroll\*.crt contoso-rca.crt
copy %windir%\system32\CertSrv\CertEnroll\contoso-rca.crt C:\CertData :: Задаём
срок действия издаваемых сертификатов
certutil -setreg CA\ValidityPeriodUnits 15
certutil -setreg CA\ValidityPeriod "Years" :: Задаём время жизни списков отзыва
согласно нашей конфигурации
certutil -setreg CA\CRLPeriodUnits 180
certutil -setreg CA\CRLPeriod "Days"
certutil -setreg CA\CRLOverlapPeriod "Months"
certutil -setreg CA\CRLOverlapUnits 1 :: Отключаем дифференциальные списки отзыва
(или Delta CRL)
certutil -setreg CA\CRLDeltaPeriodUnits 0 :: Отключаем генерацию кросс-
сертификатов
certutil -setreg ca\CRLFlags +CRLF_DISABLE_ROOT_CROSS_CERTS :: Конфигурируем ЦС
для включения истёкших отозванных сертификатов в списки отзыва
certutil -setreg ca\CRLFlags +CRLF_PUBLISH_EXPIRED_CERT_CRLS :: Включаем полный
аудит событий на ЦС**
certutil -setreg CA\AuditFilter 127 :: если версия ОС ниже, чем Windows Server
2016 необходимо задать алгоритм подписи.
:: Windows Server 2016 по умолчанию использует SHA256.
Certutil -setreg ca\csp\CNGHashAlgorithm SHA256 :: Перезапускаем службу ЦС для
применения изменений.
net stop certsvc && net start certsvc :: Публикуем списки отзыва.
certutil -CRL

```

Ряд команд нуждается в более развёрнутом пояснении. Команды с настройкой расширений CRL Distribution Points и Authority Information Access имеют специфический синтаксис. Во-первых, пути публикации и распространения указываются в одну строку и разделяются символом новой строки «\n». Каждый путь начинается с числа и отделяется от самого пути символом двоеточия. Это число в

начале пути указывает битовую маску флагов публикации для конкретного пути. Значение каждого бита для расширений CDP и AIA приведено в следующей таблице:

Название галочки в MMC	Числовое значение	Название галочки в MMC	Числовое значение
Publish CRLs to this location.	1	Include in the AIA extension of issued certificates.	2
Include in the CDP extension of issued certificates.	2	Include in the Online Certificate Status Protocol (OCSP) extension.	32
Include in CRLs. Clients use this to find Delta CRL locations.	4		
Include in all CRLs. Specifies where to publish in AD DS when publishing manually.	8		
Publish Delta CRLs to this location.	64		
Include in the IDP extension of issued CRLs.	128		

Если взять путь для CDP: 1:%windir%\system32\CertSrv\CertEnroll\%%3%%8.crl, то цифра 1 в начале строки говорит о том, что это путь физического размещения файла (Publish CRLs to this location). Другие опции здесь не используются. Для включения пути, который будет публиковаться в издаваемых сертификатах, мы будем использовать опцию «Include in the CDP extension of issued certificates» с числовым значением 2. Такой же принцип применяется и для остальных путей. В каждом пути включены переменные с двойным знаком процента «%%». Это переменные, которые ЦС при формировании пути будет автоматически заполнять исходя из типа переменной.

Первый знак процента используется как эскейп-символ, чтобы процессор командной строки воспринял следующий знак процента как литерал. Дело в том, что знак процента в командном процессоре CMD является служебным символом. Сервер ЦС так же использует знак процента для указания, что это переменная. Для исключения конфликта в командном процессоре используется последовательность из двух знаков процента.

Следующая таблица содержит описание всех доступных переменных и их краткое описание:

Переменная в редакторе расширений CDP и AIA	Переменная в скрипте	Где используется	Значение
<ServerDNSName>	%1	CDP/AIA	Полное ДНС имя сервера ЦС
<ServerShortName>	%2	CDP/AIA	Короткое (NetBIOS) имя сервера ЦС
<CaName>	%3	CDP/AIA	Имя ЦС (атрибут CN в сертификате)
<CertificateName>	%4	AIA	Индекс сертификата ЦС. Используется только при обновлении сертификата ЦС.
<ConfigurationContainer>	%6	CDP/AIA	Путь к configuration naming context в Active Directory
<CATruncatedName>	%7	CDP/AIA	Укороченное (санитизированное) имя сертификата ЦС. В общем случае будет совпадать с полным именем ЦС
<CRLNameSuffix>	%8	CDP	Индекс ключа ЦС, которым был подписан данный CRL. Используется при обновлении ключевой пары ЦС.
<DeltaCRLAllowed>	%9	CDP	Добавляет суффикс для Delta CRL (знак «+»).
<CDPObjectClass>	%10	CDP	Класс объекта в Active Directory
<CAObjectClass>	%11	CDP/AIA	Класс объекта в Active Directory

В нашем конкретном случае будут использоваться только две переменные: <CertificateName> и <CRLNameSuffix>. Для исходного сертификата ЦС эти переменные пустые. При обновлении сертификата ЦС, переменная будет заменяться на «(index)», где index — номер сертификата ЦС. Индексирование начинается с нуля. Например, имя файла для последующего сертификата ЦС будет иметь вид: contoso-rca(1).crt. И так далее. То же самое касается и переменной , только здесь будет указываться индекс ключевой пары ЦС. Отдельного внимания

заслуживает команда, которая включает аудит операций на сервере ЦС, которые регистрируются в системном журнале Security.evtx. К ним относятся все основные операции: запуск/остановка службы, отправление запроса, выпуск или отклонение сертификата, выпуск списка отзыва. Эту строчку можно найти практически в каждом постустановочном скрипте для ЦС, которые можно найти в похожих статьях в интернете. И практически никто не утруждает себя в подробном объяснении механизма его работы, просто копируют из статьи в статью. Особенность ведения аудита ЦС заключается в том, что настройка флагов аудита на ЦС является необходимым, но не достаточным условием. Механизм аудита основан на регистрации событий в журнале Security.evtx, который, в свою очередь зависит от настройки политики Audit Object Access в групповых политиках. Т.е. без настройки групповых политик никакого аудита не будет. Опытные администраторы знают к чему приводит включение Audit Object Access — к лавинному созданию записей в журнале от других компонентов ОС. Например, аудит доступа файловой системы, реестра, других установленных ролей и т.д. В результате, журнал может буквально за день-два заполниться до отказа. Поэтому для эффективного использования аудита необходимы меры по фильтрации ненужных событий, например, при помощи функции подписки на интересующие события. Нет смысла в аудите, если его никто не может прочитать и эффективно проанализировать. Но эта тема уже выходит за рамки этой статьи.

Прочие настройки

После того как корневой ЦС установлен и сконфигурирован, убедитесь, что всё прошло без ошибок:

- Откройте оснастку Certification Authorities MMC (certsrv.msc), убедитесь, что служба запущена;
- Выберите свойства узла ЦС и проверьте поля сертификата, что они соответствуют ожидаемым значениям;
- Найдите в корне системного диска папку CertData и убедитесь, что там находится два файла: сертификат и список отзыва. Убедитесь, что поля списка отзыва соответствуют ожидаемым значениям.

Если всё хорошо, тогда скопируйте содержимое папки C:\CertData на сервер IIS в папку PKIData. Сертификат корневого ЦС уже можно импортировать на все устройства, которые будут использовать нашу PKI. Для импорта сертификата на доменные клиенты, достаточно загрузить его в Active Directory и после обновления групповых политик на клиентах, сертификат будет установлен в локальные хранилища сертификатов во всём лесу. Для публикации сертификата в AD необходимо выполнить следующую команду:

```
Certutil -f -dspublish path\contoso-rca.crt RootCA
```

Для установки сертификата на клиентах в рабочих группах и мобильные устройства необходимо воспользоваться другими инструментами, которые есть в вашем распоряжении. Например, System Center Configuration Manager или Mobile Device Management. Если подходящих инструментов нет, можно копировать и устанавливать сертификат на компьютеры при помощи утилиты certutil.exe. Для установки сертификата в локальное хранилище сертификатов выполните следующую команду:

```
Certutil -f -addstore Root path\contoso-rca.crt
```

Установка издающего ЦС

Как и в случае с корневым ЦС, установка издающего ЦС включает в себя четыре этапа:

1. Подготовка предустановочных конфигурационных файлов (CAPolicy.inf);
2. Установка компонента ЦС;
3. Выполнение постустановочной конфигурации;
4. Проверка установки и конфигурации.

Предустановочная конфигурация

Если для корневого ЦС предустановочный конфигурационный файл нам не требовался, то для издающего ЦС он понадобится. В нём мы настроим расширения Certificate Policies и Basic Constraints для сертификата ЦС. Если с политиками всё понятно, то в расширении Basic Constraints мы запретим выдачу сертификатов другим ЦС с издающего ЦС, поскольку у нас двухуровневая иерархия и добавление новых уровней только усложняет нашу структуру и увеличивает время, затрачиваемое на проверку сертификатов клиентами. Также отключим автоматическую загрузку шаблонов из Active Directory в список выдаваемых шаблонов. По умолчанию, сервер ЦС загружает на выдачу некоторый набор шаблонов сертификатов. Это вредно по двум причинам:

1. Контроллеры домена практически мгновенно обнаруживают появление ЦС в лесу и даже при отключённой политике автоматической выдачи сами запрашивают себе сертификаты.
2. Администраторы сами должны определять какие шаблоны будут использовать в организации.

Поэтому мы сконфигурируем ЦС так, что список шаблонов к выдаче будет пустым.

Это возможно сделать только через CAPolicy.inf. В нашем случае он будет иметь следующее содержимое:

```
; заголовок INI файла
[Version]
Signature= "$Windows NT$" ; указываем список политик, которые будут включены в
сертификат ЦС. В нашем
; случае будет одна политика под названием AllIssuancePolicies.
[PolicyStatementExtension]
Policies = AllIssuancePolicy
; конфигурируем детали самой политики. Ссылку на документ Certificate Practice
; Statement (CPS) и объектный идентификатор политики
[AllIssuancePolicy]
URL = http://cdp.contoso.com/pki/contoso-cps.html
OID = 2.5.29.32.0
[BasicConstraintsExtension]
IsCA = True
PathLegth = 0
IsCritical = True
; секция прочих настроек ЦС
[certsrv_server]
; отключаем автоматическую загрузку шаблонов сертификатов для выдачи
LoadDefaultTemplates = 0
```

Файл с именем CAPolicy.inf необходимо скопировать в системную папку Windows до установки ЦС.

Установка компонента ЦС

Прежде всего необходимо добавить установочные компоненты для AD CS:

```
Install-WindowsFeature -Certificate, ADCS-Cert-Authority -IncludeManagementTools
```

После этого посмотрим на установочную таблицу, чтобы определить параметры установки:

Название параметра	Значение параметра
Сервер ЦС	
Класс ЦС	Enterprise CA
Тип ЦС	Subordinate CA
Автоматическая загрузка шаблонов	Нет
Сертификат	
Имя сертификата	Contoso Lab Issuing Certification authority

Дополнительный суффикс	OU=Division Of IT, O=Contoso Pharmaceuticals, C=US
Провайдер ключа	RSA#Microsoft Software Key Storage Provider
Длина ключа	4096 бит
Алгоритм подписи	SHA256
Срок действия	15 лет (определяется вышестоящим ЦС)
Политики выдачи	1) Имя: All Issuance Policies OID=2.5.29.32.0 URL=http://cdp.contoso.com/pki/contoso-cps.html
Basic Constraints	isCA=True (тип сертификата — сертификат ЦС) PathLength=0 (запрещается создание других промежуточных ЦС под текущим ЦС).

В таблице я выделил только те параметры, которые задаются в процессе установки. Остальные параметры будут настраиваться после установки. Исходя из этих данных сформируем параметры для командлета [Install-AdcsCertificationAuthority](#):

```
Install-AdcsCertificationAuthority -CACommonName "Contoso Lab Issuing
Certification authority" `
  -CADistinguishedNameSuffix "OU=Division Of IT, O=Contoso Pharmaceuticals,
C=US" `
  -CAType EnterpriseSubordinateCa `
  -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
  -KeyLength 4096 `
  -HashAlgorithmName SHA256
```

После выполнения этой команды будет выведено сообщение о том, что установка ЦС не завершена и для её завершения необходимо отправить сгенерированный запрос (находится в корне системного диска) на вышестоящий ЦС и получить подписанный сертификат. Поэтому находим файл с расширением «.req» в корне системного диска и копируем его на корневой ЦС и на корневом ЦС выполняем следующие команды:

```
# отправляем запрос на ЦС.
certreq -submit 'C:\CA-01.contoso.com_Contoso Lab Issuing Certification
authority.req'
# предыдущая команда выведет номер запроса. Укажите этот номер запроса в следующей
команде
# в моём случае это номер 2
certutil -resubmit 2
# после выпуска сертификата сохраните его в файл. При этом укажите тот же самый
номер
# запроса, который был указан после выполнения первой команды
certreq -retrieve 2 C:\subca.crt
```

Полученный файл (subca.crt) необходимо скопировать обратно на издающий ЦС и завершить инсталляцию:

```
certutil -installcert c:\subca.crt
net start certsvc
```

Мы устанавливаем на ЦС выписанный сертификат и запускаем службу сертификатов. После успешной установки можно запустить оснастку Certification Authorities MMC (certsrv.msc) и убедиться, что сертификат успешно установлен и ЦС в работающем состоянии. Теперь осталось дело за постустановочной конфигурацией.

Итоговая настройка

По аналогии с корневым ЦС, нам потребуется сконфигурировать ряд параметров на издающем ЦС. Для этого мы снова напишем BATCH скрипт с использованием утилиты certutil.exe. Но прежде всего посмотрим установочную таблицу и выясним параметры, которые нам необходимо настроить: Аналогичная таблица составляется и для издающего ЦС.

Название параметра	Значение параметра
Сервер ЦС	
Срок действия издаваемых сертификатов	Максимально: 5 лет (остальное контролируется шаблонами сертификатов)
Публикация в AD (контейнеры)	AIA NTAuthCertificates
Состав CRL	Base CRL Delta CRL
Точки публикации CRT	1) По-умолчанию 2) \\IIS\PKI\contoso-pica<CertificateName>.crt
Точки распространения CRT	1) cdp.contoso.com/pki/contoso-pica <CertificateName>.crt
Точки публикации CRL	1) По-умолчанию 2) \\IIS\PKI\contoso-pica<CRLNameSuffix><DeltaCRLAllowed>.crl
Точки распространения CRL	1) cdp.contoso.com/pki/contoso-pica <CRLNameSuffix><DeltaCRLAllowed>.crl
Base CRL	
Тип	Base CRL

Срок действия	1 неделя
Расширение срока действия	По умолчанию
Алгоритм подписи	SHA256
Публикация в AD	Нет
Delta CRL	
Тип	Delta CRL
Срок действия	1 день
Расширение срока действия	По-умолчанию
Алгоритм подписи	SHA256
Публикация в AD	Нет

За основу мы возьмём скрипт с корневого ЦС и изменим только отдельные фрагменты:

```

:.....
:
:
:
:.....
:
: все комментарии помечены знаком двойного двоеточия (:)
: записываем пути для публикации и распространения сертификатов ЦС и списков
отзыва
: в отдельные переменные
SET CrlLocal=\\IIS\PKI\contoso-pica%8%9.crl
SET CDP=http://cdp.contoso.com/pki/contoso-pica%8%9.crl
SET AIA=http://cdp.contoso.com/pki/contoso-pica%4.crt :: Настраиваем пути
публикации и распространения для сертификатов ЦС и списков отзыва.
certutil -setreg CA\CRLPublicationURLs
"1:%windir%\system32\CertSrv\CertEnroll\%3%8%9.crl\n65:CrlLocal\n6:CDP%" cer
tutil -setreg CA\CACertPublicationURLs
"1:%windir%\system32\CertSrv\CertEnroll\%1_%3%4.crt\n2:AIA%" :: Поскольку мы
не можем указывать пути публикации для файла сертификата, мы
:: вручную переименовываем его в необходимый формат и копируем в сетевую папку
ren %windir%\system32\CertSrv\CertEnroll\*.crt contoso-pica.crt
copy %windir%\system32\CertSrv\CertEnroll\contoso-pica.crt \\IIS\PKI :: Задаём
срок действия издаваемых сертификатов
certutil -setreg CA\ValidityPeriodUnits 5
certutil -setreg CA\ValidityPeriod "Years" :: Задаём время жизни списков отзыва
согласно нашей конфигурации
:: базовый CRL
certutil -setreg CA\CRLPeriodUnits 1
certutil -setreg CA\CRLPeriod "weeks" :: Delta CRL
certutil -setreg CA\CRLDeltaPeriodUnits 1
certutil -setreg CA\CRLDeltaPeriod "days" :: Включаем полный аудит событий на ЦС**
certutil -setreg CA\AuditFilter 127 :: Включаем наследование расширения
Certificate Policies в издаваемых сертификатах
certutil -setreg Policy\EnableRequestExtensionList +"2.5.29.32" :: Включаем
поддержку расширения OcspRevNoCheck, если планируется установка
:: сетевого ответчика (Online Responder или OCSP сервера)
certutil -v -setreg policy\editflags +EDITF_ENABLEOCSPREVNOCHECK :: если версия ОС
ниже, чем Windows Server 2016 необходимо задать алгоритм подписи.
:: Windows Server 2016 по умолчанию использует SHA256.
Certutil -setreg ca\csp\CNGHashAlgorithm SHA256 :: Перезапускаем службу ЦС для
применения изменений.
net stop certsvc && net start certsvc :: Публикуем списки отзыва.
certutil -CRL

```

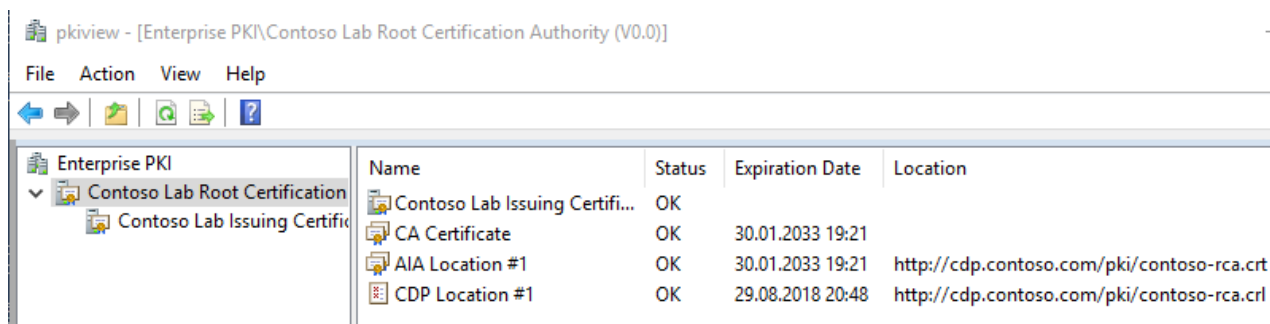
Заметим, что в путях CRLDistribution Points, изменены флаги публикации (добавлена публикация Delta CRL) и добавлена переменная %9 в имя файла для поддержки уникального имени для дельты. Здесь мы больше не создаём папку в корне системного диска, а используем сетевую папку PKI на сервере IIS, куда напрямую копируем файл сертификата и публикуем списки отзыва.

Прочие настройки

После того как издающий ЦС установлен и сконфигурирован, убедитесь, что всё прошло без ошибок:

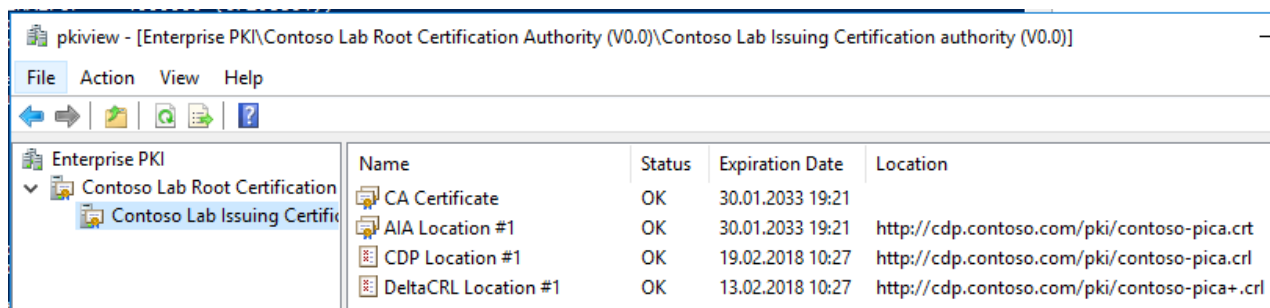
- Откройте оснастку **Certification Authorities MMC** (certsrv.msc), убедитесь, что служба запущена
- Выберите свойства узла ЦС и проверьте поля сертификата, что они соответствуют ожидаемым значениям.
- Откройте сетевую папку PKI (на сервере IIS) и убедитесь, что там есть два файла сертификата (корневого и издающего ЦС) и три списка отзыва (один для корневого, два для издающего ЦС). Убедитесь, что поля в сертификатах и списках отзыва соответствуют ожидаемым значениям.

Когда основные параметры проверены, необходимо убедиться в правильной связи иерархии ЦС и доступности всех внешних файлов для клиентов. Для этого на сервере ЦС (а лучше, на рабочей станции, где установлены средства удалённого администрирования ЦС) необходимо запустить оснастку **Enterprise PKI Health** (pkiview.msc). Оснастка автоматически построит текущую иерархию и проверит доступность всех путей для скачивания сертификатов ЦС и списков отзыва. Никаких ошибок быть не должно. Если есть ошибка, необходимо её точно идентифицировать и устранить. В случае успешной настройки оснастка будет выглядеть следующим образом для корневого ЦС:



Name	Status	Expiration Date	Location
Contoso Lab Issuing Certifi...	OK		
CA Certificate	OK	30.01.2033 19:21	
AIA Location #1	OK	30.01.2033 19:21	http://cdp.contoso.com/pki/contoso-rca.crt
CDP Location #1	OK	29.08.2018 20:48	http://cdp.contoso.com/pki/contoso-rca.crl

И для издающего ЦС:



Name	Status	Expiration Date	Location
CA Certificate	OK	30.01.2033 19:21	
AIA Location #1	OK	30.01.2033 19:21	http://cdp.contoso.com/pki/contoso-pica.crt
CDP Location #1	OK	19.02.2018 10:27	http://cdp.contoso.com/pki/contoso-pica.crl
DeltaCRL Location #1	OK	13.02.2018 10:27	http://cdp.contoso.com/pki/contoso-pica+.crl

Если вся итоговая конфигурация соответствует ожидаемым значениям и оснастка **Enterprise PKI Health** не показывает ошибок, это может судить о том, что PKI установлена верно.

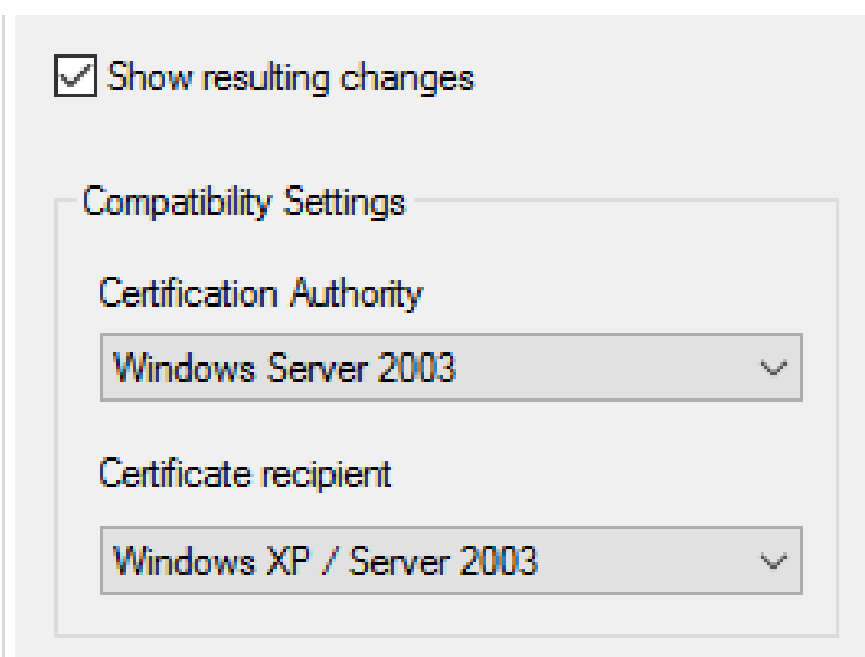
Рекомендации

После того, как все ЦС установлены, сконфигурированы и их работоспособность проверена, можно приступать к их эксплуатации. В этом разделе я дам несколько полезных рекомендаций, которых следует придерживаться, чтобы предостеречь себя от возможных потенциальных проблем во время эксплуатации PKI.

Шаблоны сертификатов

Наряду с установкой издающего ЦС, в Active Directory устанавливается набор уже готовых шаблонов сертификатов. Их можно просмотреть в оснастке **Certificate Templates MMC** (certtmpl.msc). Рекомендации по шаблонам сертификатов:

Использование готовых шаблонов сертификатов Я рекомендую использовать их копии, даже если вы не планируете вносить в них изменения. Для создания копии шаблона выберите в списке подходящий шаблон, в контекстном меню выберите **Duplicate Template** и создайте его копию. Целесообразно в имя шаблона включить название компании, чтобы отличить предустановленный шаблон от вами созданного. Например, **Contoso Web Server, Contoso Smart Card Logon**. Это позволит сравнить настройки исходного и вами созданного шаблона в случае неработоспособности шаблона. **Версия шаблона** Начиная с Windows Server 2012, интерфейс создания шаблона несколько изменился. В самом начале появляется окно с выбором версии ОС на ЦС и предполагаемом клиенте:



Если у вас используются современные версии ОС (например, Windows 7 и выше), может появиться желание выставить настройки на максимум. Если вы не уверены, что ваше приложение совместимо с CNG (Cryptography Next Generation), следует использовать настройки, которые приведены на картинке. Если выставляете ОС сервера и клиента выше, чем Windows Server 2003/Windows XP, шаблон будет использовать криптографию несовместимую с этими приложениями. Например, большинство приложений, написанных на .NET, семейство продуктов System Center,

службы федераций (AD FS) и т.д. не смогут использовать ключи таких сертификатов (но проверять смогут). Успешно такие сертификаты смогут использовать приложения, которые используют не .NET, а нативные функции CryptoAPI. К таким приложениям можно отнести, например, IIS, Remote Desktop Services. **Поля Subject и Subject Alternative Names** Существует два метода заполнения поля Subject и расширения Subject Alternative Names: автоматический и ручной. Это настраивается в настройках шаблона сертификата, во вкладке Subject Name.

The screenshot shows the 'RAS and IAS Server Properties' dialog box with the 'Subject Name' tab selected. The 'Issuance Requirements' sub-tab is also visible. The 'Build from this Active Directory information' radio button is selected, and the 'Use subject information from existing certificates for autoenrollment renewal requests (*)' checkbox is unchecked.

Superseded Templates		Extensions		Security		Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation			

Subject Name | Issuance Requirements

☐ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests (*)

☒ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Если выбран второй пункт (как на картинке), ЦС игнорирует имя субъекта из запроса сертификата и заполняет эти поля из свойств учётной записи пользователя или устройства, которое запрашивает сертификат. В ряде случаев это не подходит (например, сертификаты для внутренних веб-сайтов) и имя субъекта заполняется из значения в запросе сертификата. Тогда переключатель необходимо выставить в верхнее положение. Дополнительно к этому, на вкладке Issuance Requirements обязательно надо выставить галочку «CA certificate manager approval».

The screenshot shows the 'RAS and IAS Server Properties' dialog box with the 'Subject Name' tab selected. The 'Require the following for enrollment' section is visible, and the 'CA certificate manager approval' checkbox is checked.

Superseded Templates		Extensions		Security		Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation			

Subject Name | Issuance Requirements

Require the following for enrollment:

☒ CA certificate manager approval

Это необходимо затем, что имя для сертификата никак не проверяется. Если этот момент не контролировать, пользователь может запросить сертификаты на любое имя и скомпрометировать весь лес Active Directory. Вряд ли вы позволите рядовому пользователю получить сертификат на имя администратора. После требования одобрения запроса менеджером сертификатов на ЦС, каждый запрос с явным указанием субъекта сертификата будет попадать на ЦС в папку Pending Requests и не будет подписан, пока оператор ЦС не изучит его содержимое и не примет решение о выпуске. Т.е. каждый такой запрос необходимо вручную проверять на содержимое и убедиться, что в запросе указаны верные и допустимые имена. В противном случае запрос должен быть отклонён.

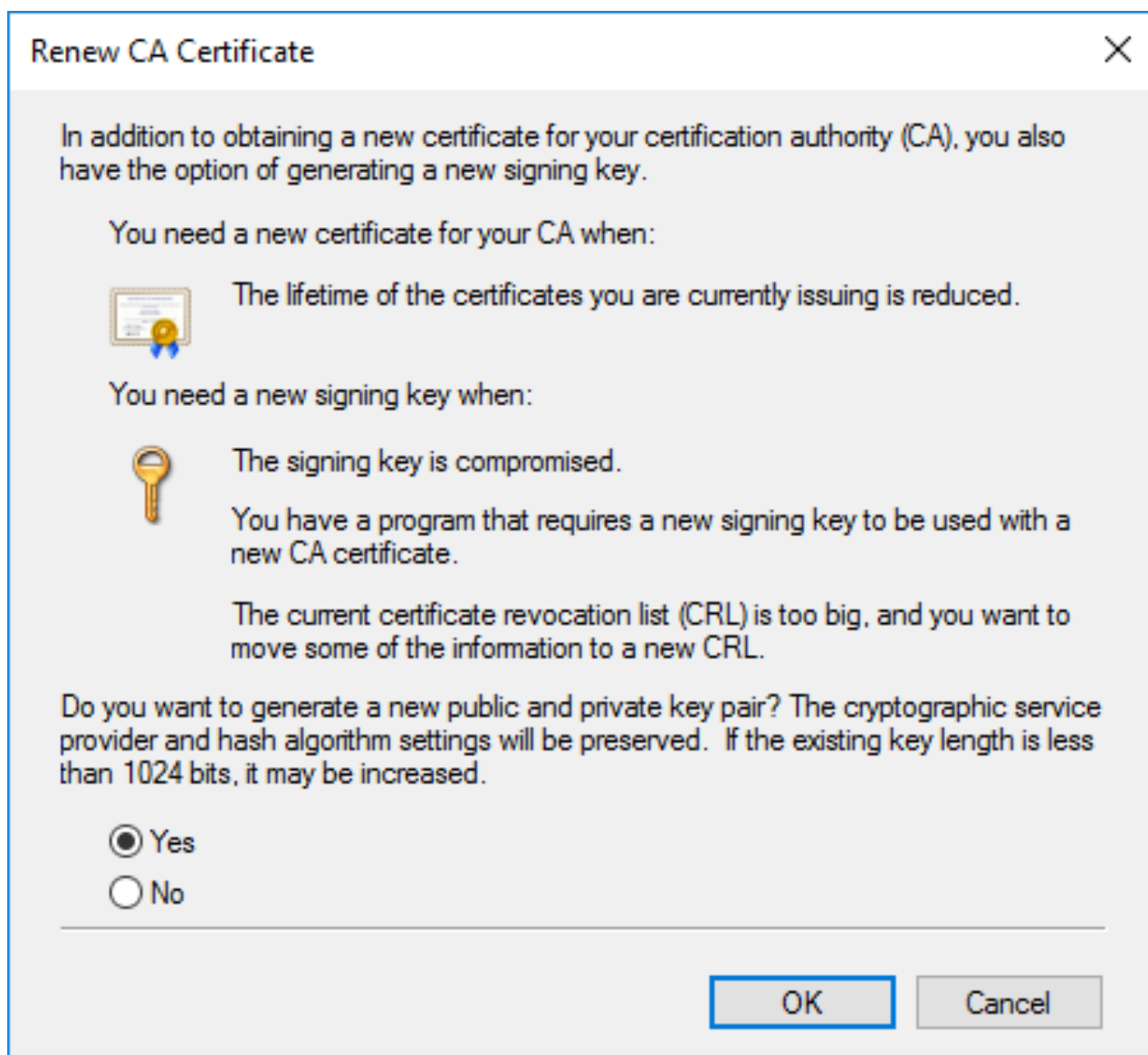
Права на шаблоны сертификатов Шаблоны сертификатов в Active Directory хранятся в разделе configuration naming context, который реплицируется между всеми контроллерами домена в лесу. Поэтому для назначения прав на шаблоны сертификатов можно использовать только глобальные и универсальные группы. Избегайте назначения прав отдельным пользователям и устройствам.

Обновление сертификатов ЦС

Периодически необходимо обновлять сертификаты ЦС. Рассмотрим несколько аспектов, связанных с обновлением сертификатов ЦС. **Периодичность обновления сертификата ЦС** Это делается в следующих случаях:

- Срок жизни сертификата ЦС истекает;
- Ключ ЦС скомпрометирован;
- Необходимо изменить длину ключа или алгоритм подписи;
- Слишком большой список отзыва (больше нескольких мегабайт).

Первый вопрос, если всё идёт штатно, за какое время до истечения срока действия сертификата ЦС его нужно обновлять? Сертификат издающего ЦС должен обновляться за максимальный срок действия издаваемых сертификатов. В нашем случае срок действия сертификата издающего ЦС 15 лет, а максимальный срок действия издаваемых сертификатов 5 лет (см. конфигурационную таблицу). Это означает, что сертификат издающего ЦС необходимо обновить через 10 лет. Если это время затянуть, то мы не сможем обеспечить необходимый срок действия для самого долгосрочного шаблона. **Порядок обновления ЦС** В нашей двухуровневой иерархии сертификаты корневого и издающего ЦС имеют одинаковый срок действия. Поэтому, когда вы принимаете решение об обновлении сертификата любого ЦС, необходимо обновлять их вместе. Первым обновляется сертификат корневого ЦС, затем сертификат издающего ЦС. **Генерация ключей при обновлении сертификатов ЦС** При обновлении сертификатов ЦС вам предлагается две опции: использовать существующую ключевую пару или сгенерировать новую:



В диалоговом окне обновления ключевой пары приведены рекомендации Microsoft по выбору ключевой пары. Однако, практика показывает, что эти рекомендации устарели. Следует всегда генерировать новую ключевую пару. При использовании нескольких сертификатов ЦС клиентский модуль построения цепочки сертификатов иногда может ошибиться и выбрать неправильный сертификат. В базе знаний Microsoft отмечены такие проблемы. Примеры статей:

- [Certificate validation fails when a certificate has multiple trusted certification paths to root CAs.](#)
- [«0x80092013, CRYPT_E_REVOCATION_OFFLINE» error message when you try to verify a certificate that has multiple chains in Windows Server 2008 or in Windows Vista.](#)

При генерации новой ключевой пары для каждого сертификата будет гарантирован только один путь к корневому сертификату и модуль построения цепочек сертификатов уже не ошибётся.

Резервное копирование

Вопросы резервного копирования и восстановления после отказа являются отдельной темой. Здесь я лишь отмечу основные моменты, которые следует учесть при планировании стратегии резервного копирования. Microsoft Active Directory Certificate Services предоставляет инструменты для резервного копирования компонентов ЦС:

- Оснастка Certification Authority MMC (certsrv.msc);
- Утилита certutil.exe с параметром -backup.

С ними можно сделать резервную копию для ключевой пары ЦС и базы данных. Однако эти инструменты не позволяют делать резервную копию настроек ЦС. Эти операции необходимо выполнять вручную. Все настройки ЦС находятся в реестре по следующему пути:

HKLM\System\CurrentControlSet\Services\CertSvc

При резервном копировании всегда экспортируйте данную ветку реестра. При восстановлении ЦС сохранённый REG файл импортируется обратно в реестр после установки роли ЦС. Полный список элементов ЦС, который подлежит обязательному резервному копированию выглядит так:

- Ключи и сертификаты ЦС;
- База данных ЦС;
- Настройки ЦС из реестра;
- Предустановочный конфигурационный файл;
- Установочные и конфигурационные скрипты.

Этот список не зависит от принятой в вашей компании стратегии резервного копирования, он всегда должен быть включён в список резервных копий.

Об авторе



Вадим Поданс — специалист в области автоматизации PowerShell и Public Key Infrastructure, Microsoft MVP: Cloud and Datacenter Management с 2009 года и автор модуля PowerShell PKI. На протяжении 9 лет в своём блоге освещает различные вопросы эксплуатации и автоматизации PKI на предприятии. Статьи Вадима о PKI и PowerShell можно найти на его [сайте](#).