Microsoft

Windows Server Managing and Supporting Active Directory Certificate Services (ADCS)

Module 4: Deploy a Two-Tier PKI Hierarchy

Microsoft Services

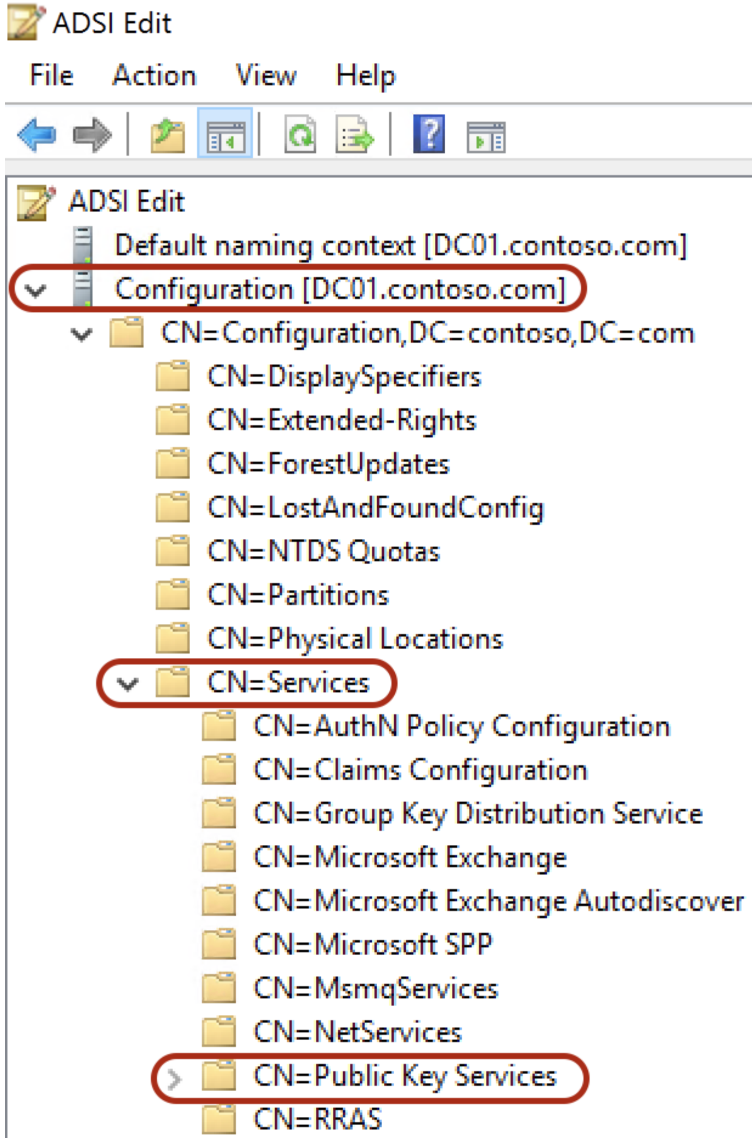
Module Overview

- PKI Objects in AD
- Planning the Revocation Infrastructure
- CA Pre-Installation Tasks
- Deploy Offline Root CA
- Deploy Subordinate Issuing CA using GUI and PowerShell
- Post-install Configuration

PKI Objects in Active Directory

Forest Configuration Container

- A PKI has no relationship to any AD
- Yet, when installing an AD integrated CA (Enterprise CA), AD will be used to store PKI related information
- This information can be used by clients to simplify certificates issue process



ADSI Edit
Default naming context [DC01.contoso.com]
Configuration [DC01.contoso.com]
CN=Configuration,DC=contoso,DC=com
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundConfig
CN=NTDS Quotas
CN=Partitions
CN=Physical Locations
CN=Services
CN=AuthN Policy Configuration
CN=Claims Configuration
CN=Group Key Distribution Service
CN=Microsoft Exchange
CN=Microsoft Exchange Autodiscover
CN=Microsoft SPP
CN=MsmqServices
CN=NetServices
CN=Public Key Services
CN=RRAS

Public Key Services Containers in AD

Object Name and Type	Description and Usage
AIA	Contains CA certificates that can be retrieved by clients using the AIA extension. Certificates in this container are also automatically retrieved by the client and stored on the “Intermediate Certificate Store”.
CDP	Contains all base CRLs and delta CRLs published in the forest.
Certificate Templates	Contains all certificate templates available in the forest.
Certification Authorities	Certificates in this container are automatically retrieved by the client and stored on the “Trusted Root Certification Authorities” store.

Public Key Services Containers in AD (cont.)

Object Name and Type	Description and Usage
Enrollment Services	For each Enterprise CA there is a corresponding pKIEnrollmentService object in this container. Clients use these objects to retrieve available certificate templates and request certificates from Enterprise CAs.
KRA	Contains the certificates for key recovery agents for the forest.
OID	Contains forest registered OIDs for PKI objects.
NTAuth Certificates (Object)	CAs issuing certificates used for authentication (e.g., Smart Card authentication) must be contained in this object. Certificates in this container are automatically retrieved by the client and stored on the “NTAuth” certificate store.

Adding related Information to AD Container

AIA

- Will be populated automatically by Enterprise CAs.
- Manual population: **certutil –dspublish –f <PathToCertFile.cer> SubCA**

CDP

- Will be populated automatically by Enterprise CAs.
- Manual population: **certutil –dspublish –f <PathToCRLFile.crl>**

Certificate Templates

- Can only be populated by using the Certificate Template Management Tool.

Certification Authorities

- Will be populated automatically by Enterprise Root CAs.
- Manual population: **certutil –dspublish -f <PathToCertFile.cer> RootCA**

Planning the Revocation Infrastructure

AIA/CDP - Stated vs Physical

- A “**Stated**” location is a URL sealed on the AIA or CDP extension of an issued certificate, where the certificate or CRL can be retrieved by the clients

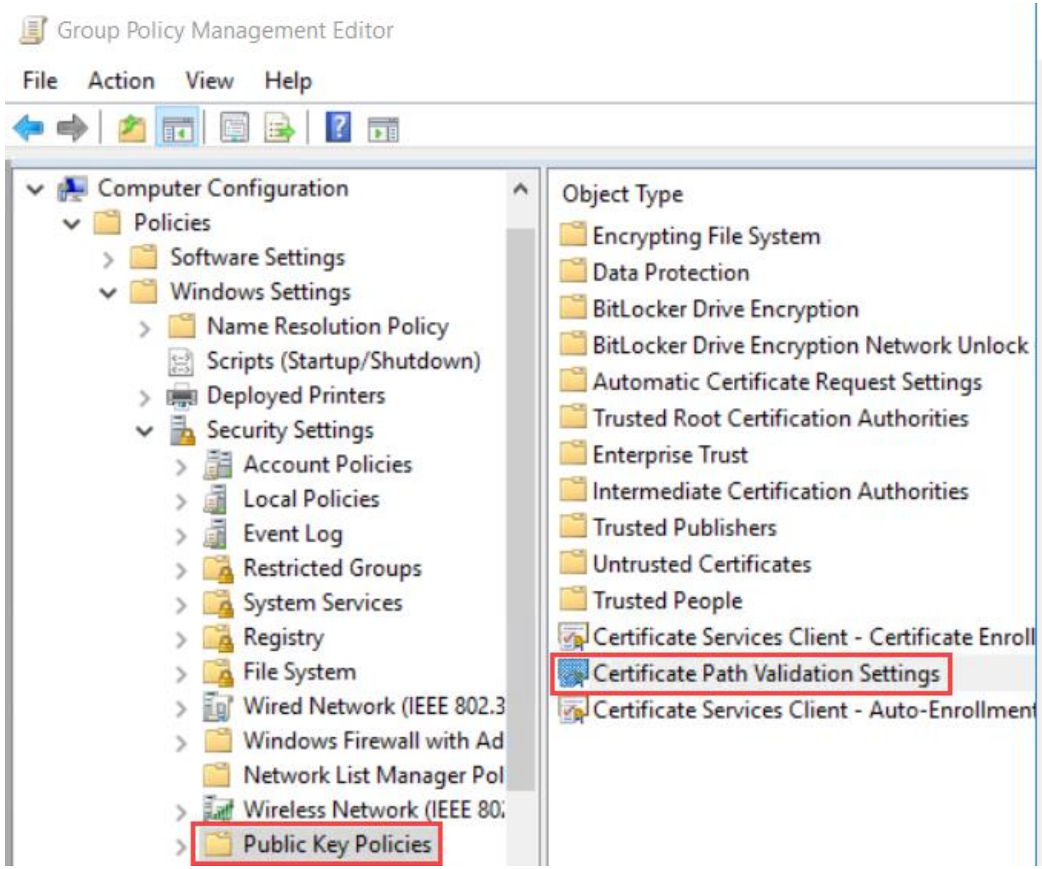
- A “**Physical**” location is where the CA or someone on behalf of the CA physically writes certificate & CRL information
  - Each CA is configured to write its certificate and CRL to a physical location (can be the same as a “stated” location)

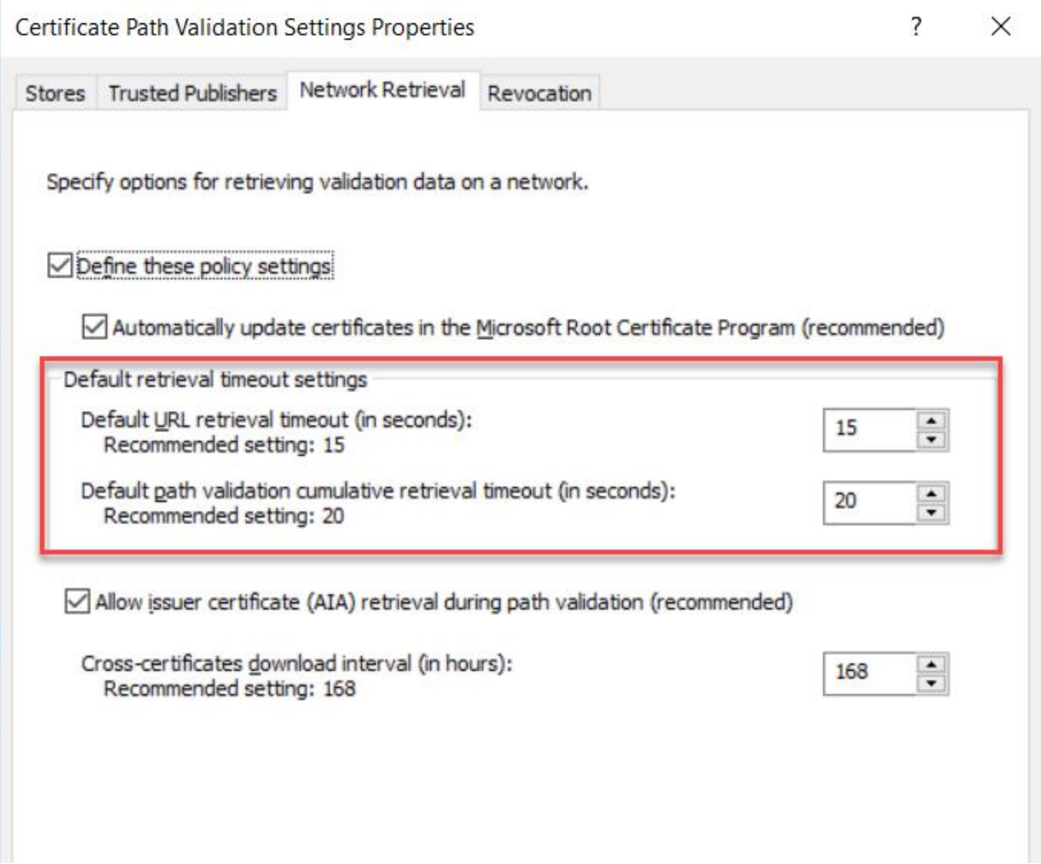
AIA/CDP - “Stated”

- Protocols Supported: LDAP, HTTP and FTP
- Hybrid approaches should be considered (i.e., both LDAP and HTTP)
- Does Order Matter: YES!
- Clients will process CDP and AIA locations in the order they are listed in the certificate

AIA/CDP - “Stated” (Cont.)

- If a client cannot access the CDP or AIA location, they will proceed to the next one after the configured retrieval timeout has been reached (**15 seconds by default**).
- You can change the default retrieval timeout by Group Policy using the setting: “**Certificate Path Validation Settings**”


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3
Windows Firewall with Ad
Network List Manager Pol
Wireless Network (IEEE 80:
Public Key Policies
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enroll
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment



Specify options for retrieving validation data on a network.

☑ Define these policy settings

☑ Automatically update certificates in the Microsoft Root Certificate Program (recommended)

Default retrieval timeout settings

Default URL retrieval timeout (in seconds): 15
Recommended setting: 15

Default path validation cumulative retrieval timeout (in seconds): 20
Recommended setting: 20

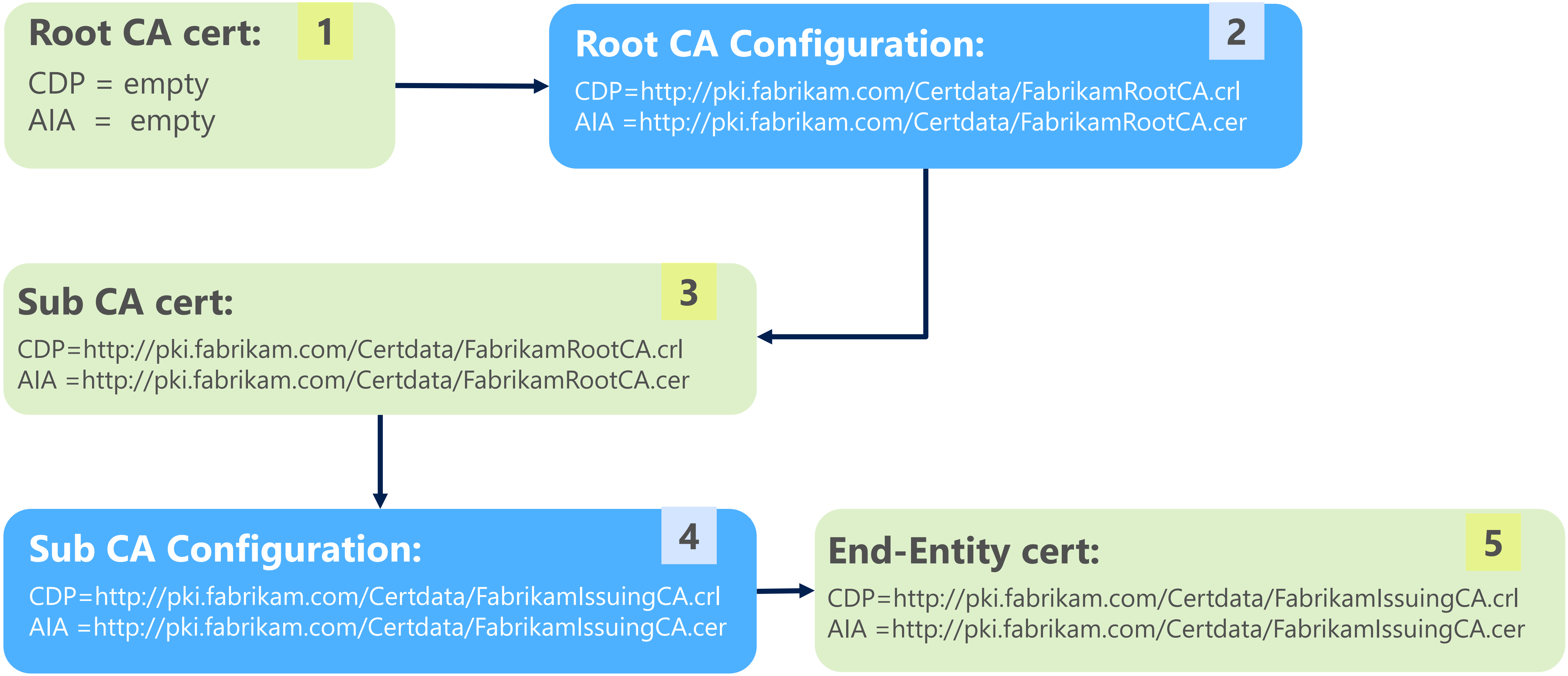
☑ Allow issuer certificate (AIA) retrieval during path validation (recommended)

Cross-certificates download interval (in hours): 168
Recommended setting: 168

AIA/CDP - “Physical”

- Manual procedure to publish offline Root CA certificate and CRL to stated (i.e., “claimed”) AIA & CDP locations
  - Published to AD using certutil
  - Published to HTTP locations via file copy
  - Publication of online Issuing CA certificate & CRL to Active Directory is automatic during deployment, certificate renewals, & CRL publications

CDP and AIA Interaction



Root CA cert: 1

CDP = empty
AIA = empty

Root CA Configuration: 2

CDP=http://pki.fabrikam.com/Certdata/FabrikamRootCA.crl
AIA =http://pki.fabrikam.com/Certdata/FabrikamRootCA.cer

Sub CA cert: 3

CDP=http://pki.fabrikam.com/Certdata/FabrikamRootCA.crl
AIA =http://pki.fabrikam.com/Certdata/FabrikamRootCA.cer

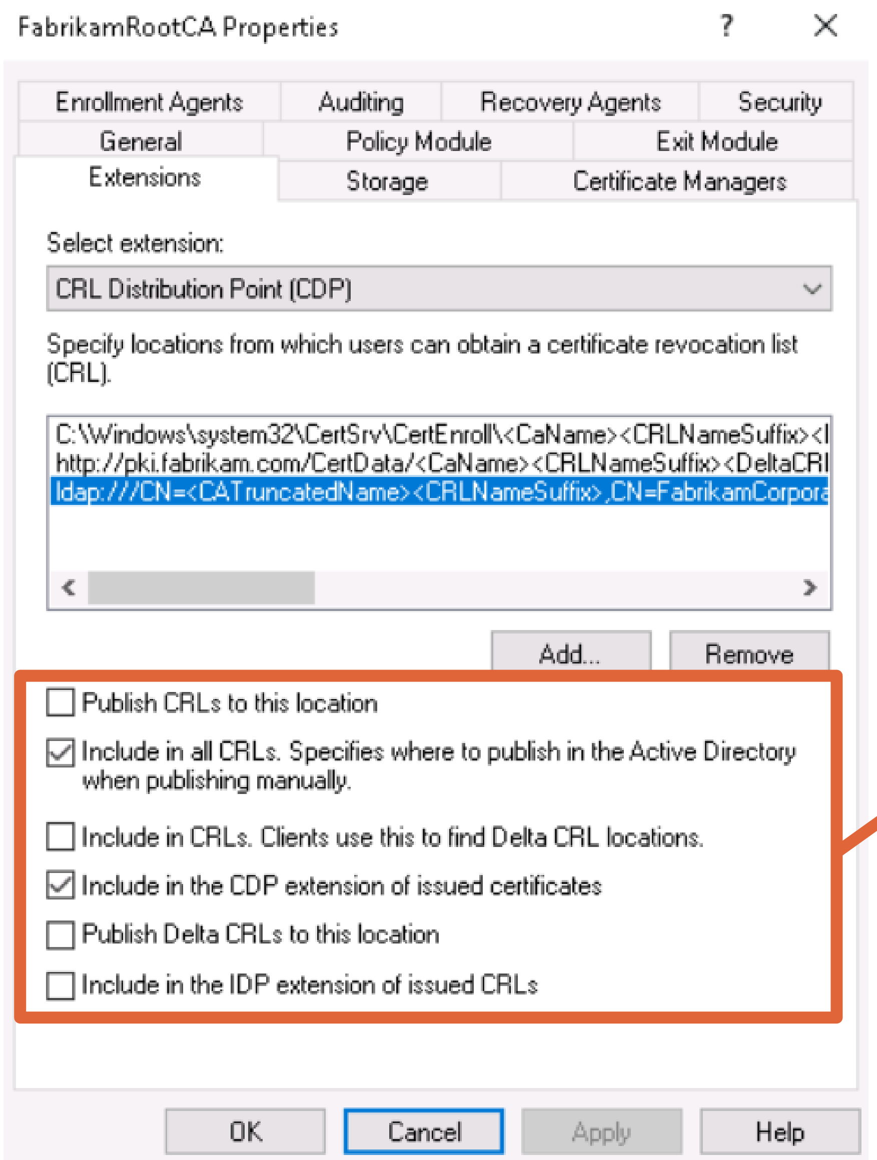
Sub CA Configuration: 4

CDP=http://pki.fabrikam.com/Certdata/FabrikamIssuingCA.crl
AIA =http://pki.fabrikam.com/Certdata/FabrikamIssuingCA.cer

End-Entity cert: 5

CDP=http://pki.fabrikam.com/Certdata/FabrikamIssuingCA.crl
AIA =http://pki.fabrikam.com/Certdata/FabrikamIssuingCA.cer

Understanding CDP Options



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><I
http://pki.fabrikam.com/CertData/<CaName><CRLNameSuffix><DeltaCRI
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=FabrikamCorpora
```

☐ Publish CRLs to this location

☑ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

☐ Include in CRLs. Clients use this to find Delta CRL locations.

☑ Include in the CDP extension of issued certificates

☐ Publish Delta CRLs to this location

☐ Include in the IDP extension of issued CRLs

1 ☐ Publish CRLs to this location

8 ☑ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

4 ☐ Include in CRLs. Clients use this to find Delta CRL locations.

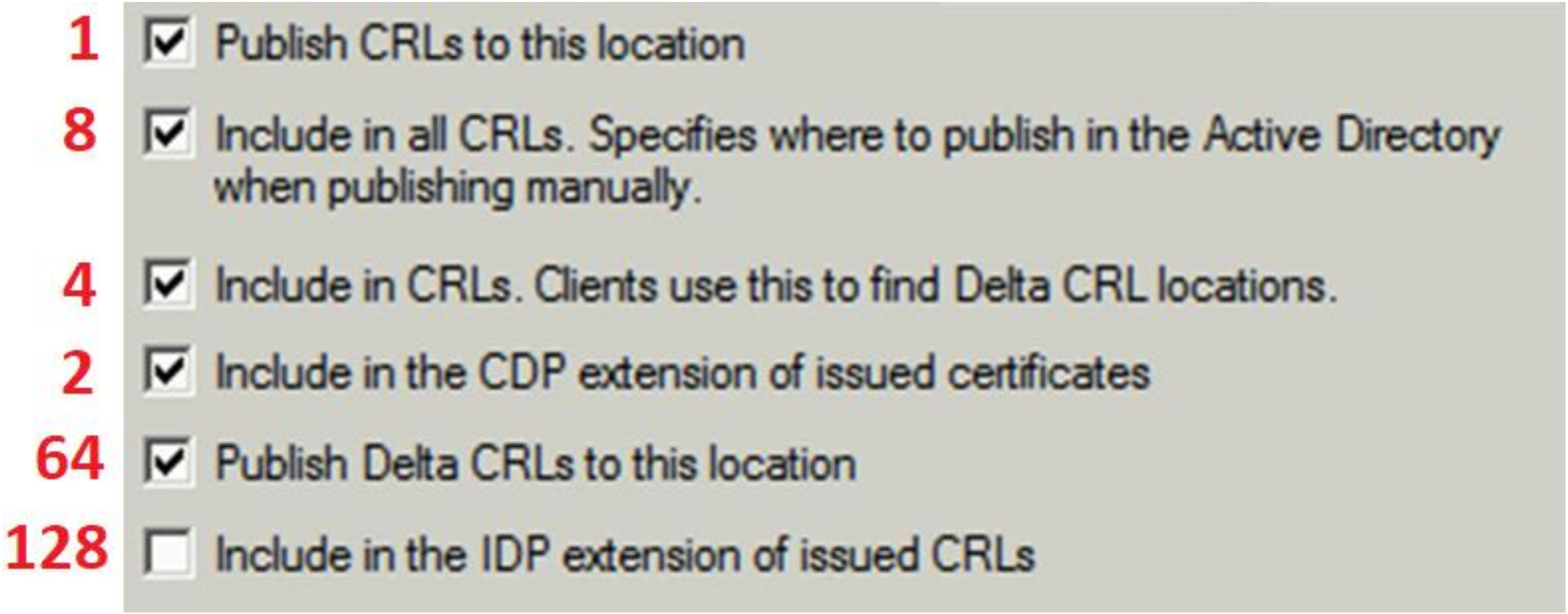
2 ☑ Include in the CDP extension of issued certificates

64 ☐ Publish Delta CRLs to this location

128 ☐ Include in the IDP extension of issued CRLs

Understanding LDAP CDP Configuration

- Default LDAP CDP:
  79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
  - The number 79 means that all checkboxes (except for the IDP) are enabled
  - The variable %2 stands for "ServerShortName"



1 ☑ Publish CRLs to this location

8 ☑ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

4 ☑ Include in CRLs. Clients use this to find Delta CRL locations.

2 ☑ Include in the CDP extension of issued certificates

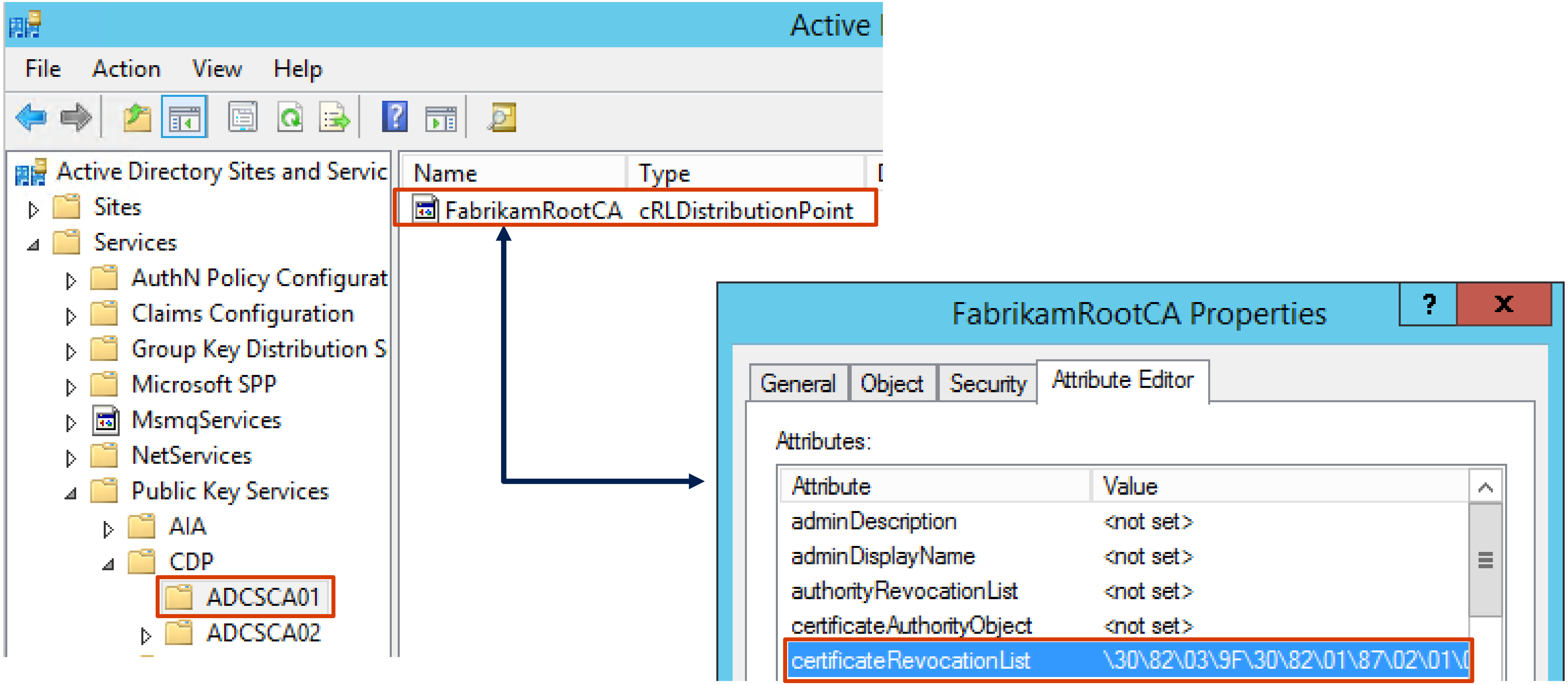
64 ☑ Publish Delta CRLs to this location

128 □ Include in the IDP extension of issued CRLs

Understanding LDAP CDP Configuration

- CDP and AIA parameters:
  - %1 = ServerDNSName
  - %2 = ServerShortName
  - %3 = SANITIZEDCANAME
  - %4 = CERTFILENAMESUFFIX
  - %5 = DOMAINDN
  - %6 = CONFIGDN
  - %7 = SANITIZEDCANAMEHASH
  - %8 = CRLFILENAMESUFFIX
  - %9 = CRLDELTAFILENAMESUFFIX
  - %10 = DSCRLATTRIBUTE
  - %11 = DSCACERTATTRIBUTE
  - %12 = DSUSERCERTATTRIBUTE
  - %13 = DSKRACERTATTRIBUTE
  - %14 = DSCROSSCERTPAIRATTRIBUTE

Understanding LDAP CDP Configuration (cont.)



Active Directory Sites and Servic
- Sites
- Services
  - AuthN Policy Configurat
  - Claims Configuration
  - Group Key Distribution S
  - Microsoft SPP
  - MsmqServices
  - NetServices
  - Public Key Services
    - AIA
    - CDP
      - ADCSCA01
      - ADCSCA02

Name	Type
FabrikamRootCA	cRLDistributionPoint

FabrikamRootCA Properties

General | Object | Security | Attribute Editor

Attributes:

Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
authorityRevocationList	<not set>
certificateAuthorityObject	<not set>
certificateRevocationList	\30\82\03\9F\30\82\01\87\02\01\(

CRL Publication Options

Display Name	Description	Label	Value
Publish CRLs to this location	Identifies locations to which the CA should automatically publish the physical CRL files	ServerPublish	1
Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually	Create an extension in the CRL file, which specifies where to publish the CRL in AD when publishing manually.	AddtoCertCDP	8
Include in CRLs. Clients use this to find delta CRL locations	Place a URL for delta CRL retrieval in a base CRL. This publication point is stored in the freshest CRL extension of a CRL, and it retrieved only during the CRL checking process	AddtoFreshestCRL	4
Include in the CDP extension of issued certificates	Place a URL in the CDP extension of a CRL issued by the CA to allow the relying party certificate chaining engine to download the latest CRL version if the current version has expired	AddtoCRLCDP	2
Publish delta CRLs to this location	If the CA is configured to enable delta CRLs, the delta CRL files are automatically published to this location	ServerPublishDelta	64
Include in the IDP extension of issued CRLs	Used by non-Windows clients to determine the scope of the CRL. The scope can include end-entity certificates only, CA certificates only, attribute certificate only, or a limited set of reason codes	IssuingDistributionPoint	128

Examples for CRL Validity Periods for the PKI

RootCA

- Validity Period: 6 Months
- Overlap Period: 2 Months

DevicesIssuingCA

- Validity Period: 5 Days
- Overlap Period: 1 Day

UserIssuingCA

- Validity Period: 2 Days
- Overlap Period: 1 Day
- Delta CRL Period: 1 Day
- Delta CRL Overlap Period: 1 Day

PKI Pre-Installation Tasks

PKI Management Groups & Accounts

CA Administrator

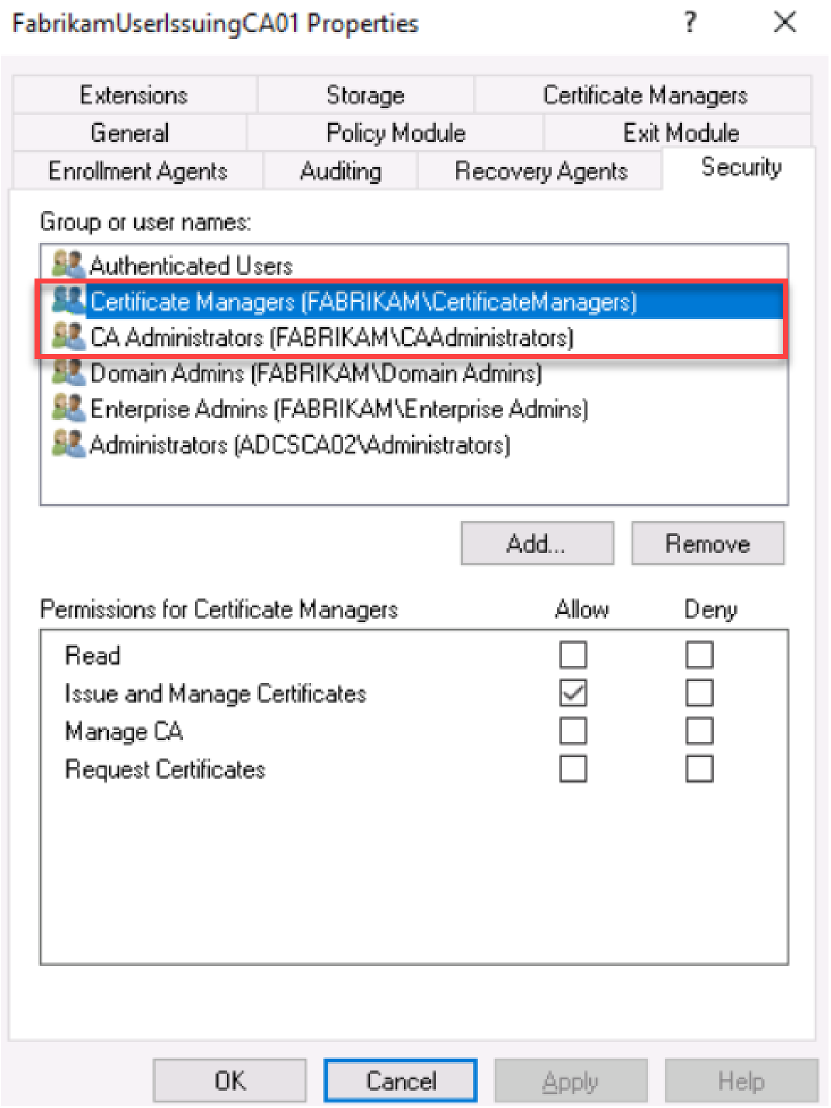
- Manage any aspect of the CA, Including Public Key Services Container
- Can restart the service
- Modify CA configuration

- CA Administrators (domain group)
- Administrators (local group)

Certificate Manager

- Manage certificate issuance
- Manage revocation issuance

- Certificate Managers (domain group)
- Administrators (local group)



FabrikamUserIssuingCA01 Properties

Group or user names:

Authenticated Users
Certificate Managers (FABRIKAM\CertificateManagers)
CA Administrators (FABRIKAM\CAAdministrators)
Domain Admins (FABRIKAM\Domain Admins)
Enterprise Admins (FABRIKAM\Enterprise Admins)
Administrators (ADCSCA02\Administrators)

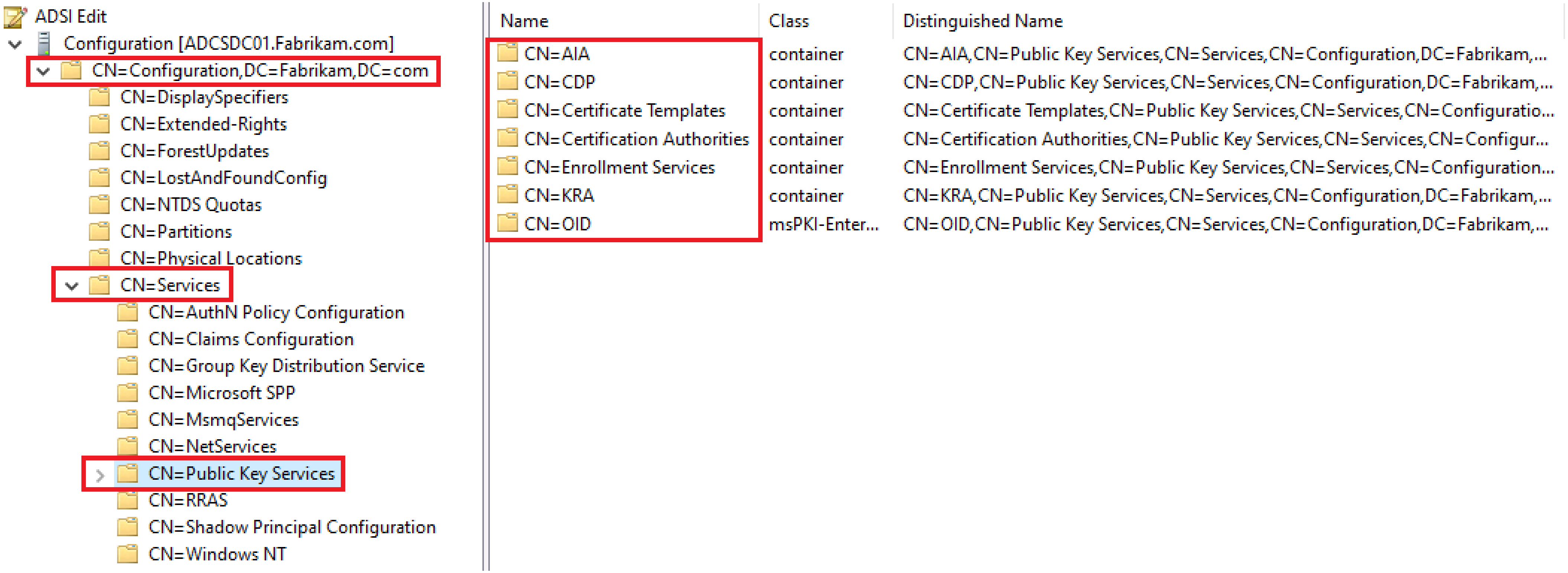
Permissions for Certificate Managers	Allow	Deny
Read	□	□
Issue and Manage Certificates	☑	□
Manage CA	□	□
Request Certificates	□	□

PKI Management Groups & Accounts

CA Administrator	Certificate Manager	Certificate Template Manager
• Manage any aspect of the CA, Including Public Key Services Container • Can restart the service • Modify CA configuration	• Manage certificate issuance • Manage revocation issuance	• Manage certificate template, including creating, modifying and deleting templates
• CA Administrators (domain group) • Administrators (local group)	• Certificate Managers (domain group) • Administrators (local group)	• Certificate Template Managers (domain group) • Custom delegation

Delegating Public Key Services Container to CA Administrators

- Provide “Full Control” permissions to the “Public Key Services” AD container
- In order to harden the management of AD CS services we only give Full permission to CA Administrators
- Domain Admin and Enterprise Admins we remove every permission except READ



```
ADSI Edit
  Configuration [ADCSDC01.Fabrikam.com]
    CN=Configuration,DC=Fabrikam,DC=com
      CN=DisplaySpecifiers
      CN=Extended-Rights
      CN=ForestUpdates
      CN=LostAndFoundConfig
      CN=NTDS Quotas
      CN=Partitions
      CN=Physical Locations
      CN=Services
        CN=AuthN Policy Configuration
        CN=Claims Configuration
        CN=Group Key Distribution Service
        CN=Microsoft SPP
        CN=MsmqServices
        CN=NetServices
        CN=Public Key Services
        CN=RRAS
        CN=Shadow Principal Configuration
        CN=Windows NT
```

Name	Class	Distinguished Name
CN=AIA	container	CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=Fabrikam,...
CN=CDP	container	CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=Fabrikam,...
CN=Certificate Templates	container	CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuratio...
CN=Certification Authorities	container	CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configur...
CN=Enrollment Services	container	CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration...
CN=KRA	container	CN=KRA,CN=Public Key Services,CN=Services,CN=Configuration,DC=Fabrikam,...
CN=OID	msPKI-Enter...	CN=OID,CN=Public Key Services,CN=Services,CN=Configuration,DC=Fabrikam,...

Lab

Module 4, Lab 1 Exercise 1:

Establish PKI Deployment Pre-requisites

Duration: 30 Minutes

Lesson Review

Question 1:

Why we created a new Web Site on the IIS Server?

In order to publish Revocation Information

Question 2:

Which group has full permission on Public Key Services Container?

CA Administrators

Question 3:

Which are the 3 primary AD Groups that Responsible AD CS infrastructure?

CA Administrator

Certificate Manager

Certificate Template Manager

Lab

Module 4, Lab 1 Exercise 2:

Question 1:

As part of the exercise, we configured the IIS Request Filtering options and enabled ‘Double escaping’. Why we did it?

To support the delta CRL file name, which, by default, ended with a ‘+’.

Question 2:

What is the purpose of ‘Cert Publishers’ group, and who is a member of this group by default?

The purpose of ‘Cert Publishers’ group is to publish certificates to Active Directory. By default, the Certificate Authority computer accounts from same domain are members in this group.

Offline Root CA

Install and Configure Offline Root CA

- An offline Root CA has to be truly offline:
  - Should never be attached to a network
  - Service Packs/Cumulative Updates should be deployed offline
  - Secure location (secured server rack, special virtualization environment)
- Pay attention that:
  - CA common name and domain membership status cannot be changed without uninstalling CA
  - Machine name can be changed during migration or when required

Define CAPolicy.inf File

- Optional configuration file that defines settings which cannot be specified using the GUI
  - Does not exist by default
  - Has to be manually copied to **%windir%**\capolicy.inf **prior to setup**

- May contain the following settings:
  - Policies to be included in the CA certificate
  - Constraints to be included in the CA certificate
  - CA certificate renewal settings
  - (Delta) CRL validity settings
  - Do not load default templates switch

Root CA: Post-Install Configuration

1. Define CRL publication intervals
2. Define CDP and AIA URLs (change defaults to appropriate HTTP and/or LDAP URLs)
3. Configure CA auditing
4. Define validity period for certificates
5. Restart AD CS service
6. Publish new CRL
7. Make CRL and AIA distribution points available:
   a. Copy the CRL and AIA to the Web Server
   b. Publish the CRL and AIA to AD

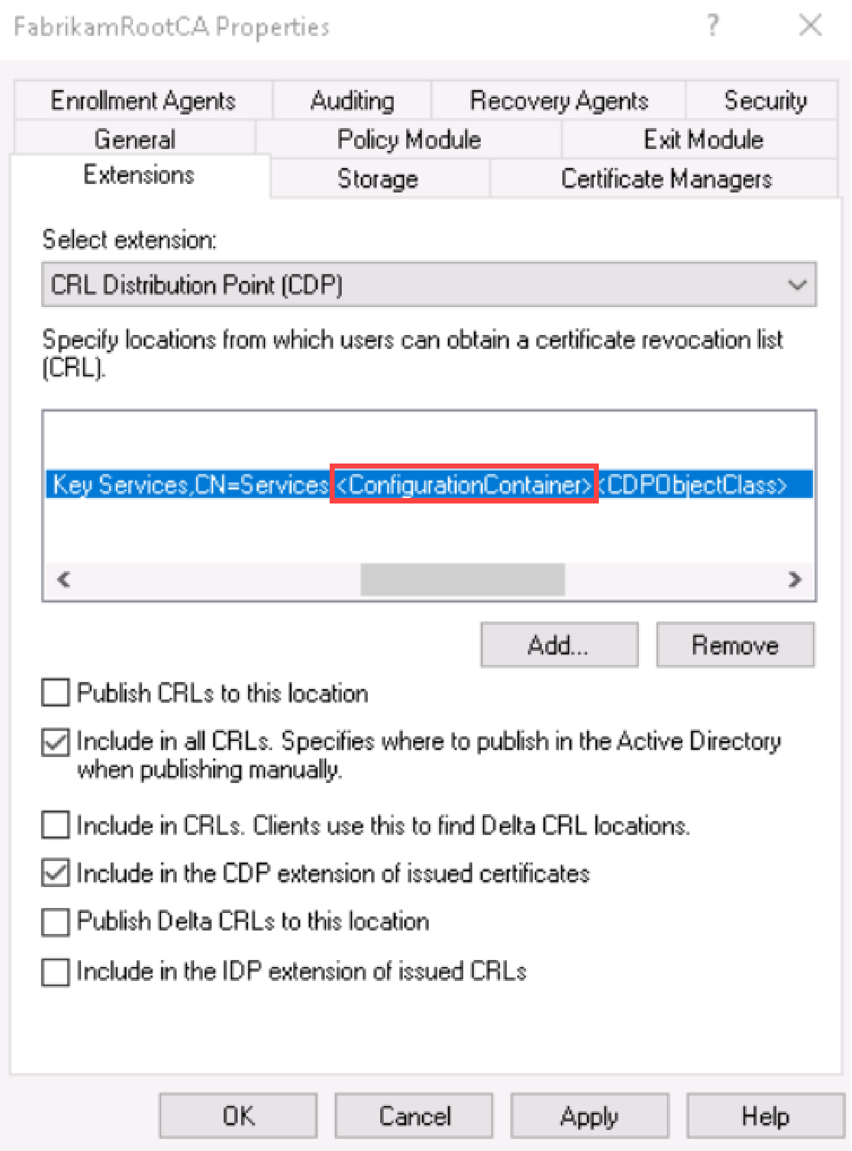
Configure DSConfigDN for LDAP CDP

- We decided to publish the Offline Root CA's CRL to Active Directory

- Because the Root CA is a standalone CA (not joined to a domain), it cannot translate the '**ConfigurationContainer**' variable (%6) in the CDP to the configuration partition DN (e.g. "CN=Configuration,DC=Fabrikam,DC=com")

- To enable the Root CA to translate 'ConfigurationParition' correctly, **DSConfigDN** value will be configured:

  Certutil -setreg CA\DSConfigDN "CN=Configuration,DC=fabrikam,DC=com"



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

Key Services,CN=Services<ConfigurationContainer><CDPObjectClass>

□ Publish CRLs to this location

☑ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

□ Include in CRLs. Clients use this to find Delta CRL locations.

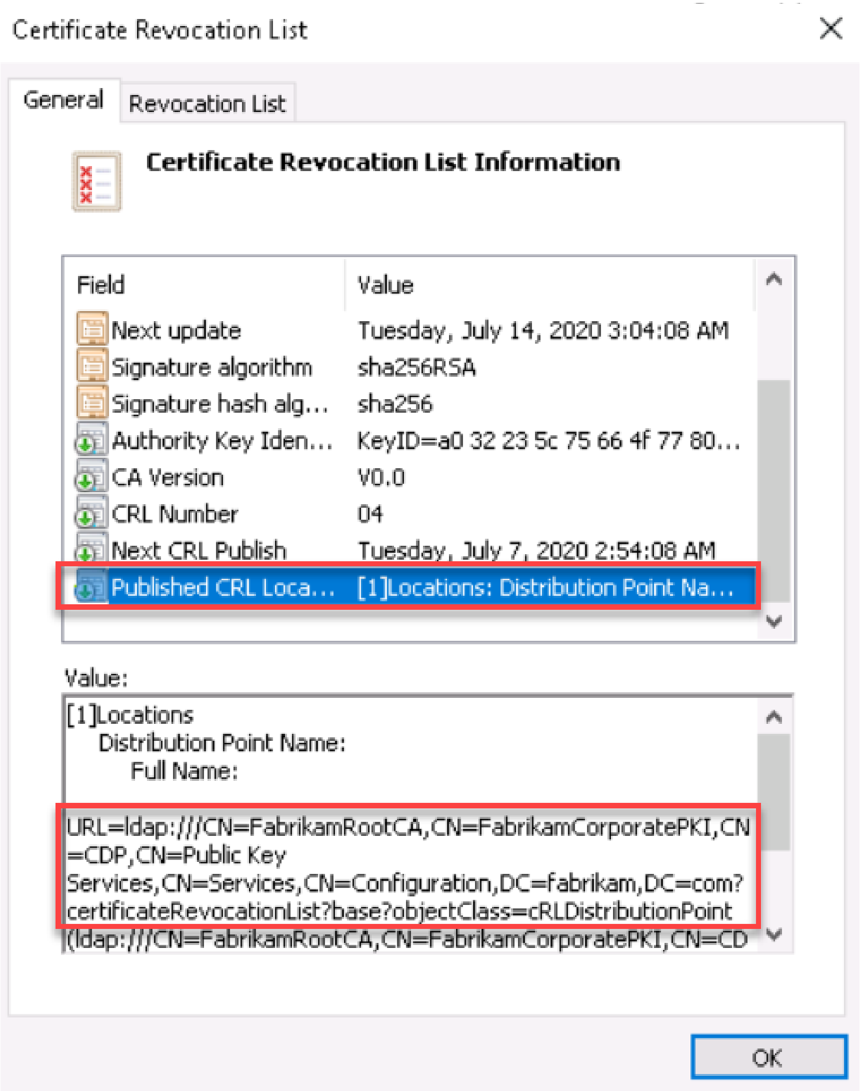
☑ Include in the CDP extension of issued certificates

□ Publish Delta CRLs to this location

□ Include in the IDP extension of issued CRLs

“Include in all CRLs” Option

- From the same reasons, the Root CA won’t be able to publish the CRL to Active Directory automatically, and we will have to do it manually using certutil –dspublish
- To make this process a bit easier, we decided to add the **Published CRL Locations** extension to the CRL, which specifies where to publish the CRL in AD when publishing manually using certutil -dspublish.
- The Published CRL Locations extension was added by enabling the “Include in all CRLs” option in the CDP.



Certificate Revocation List Information

Field	Value
Next update	Tuesday, July 14, 2020 3:04:08 AM
Signature algorithm	sha256RSA
Signature hash alg...	sha256
Authority Key Iden...	KeyID=a0 32 23 5c 75 66 4f 77 80...
CA Version	V0.0
CRL Number	04
Next CRL Publish	Tuesday, July 7, 2020 2:54:08 AM
Published CRL Loca...	[1]Locations: Distribution Point Na...

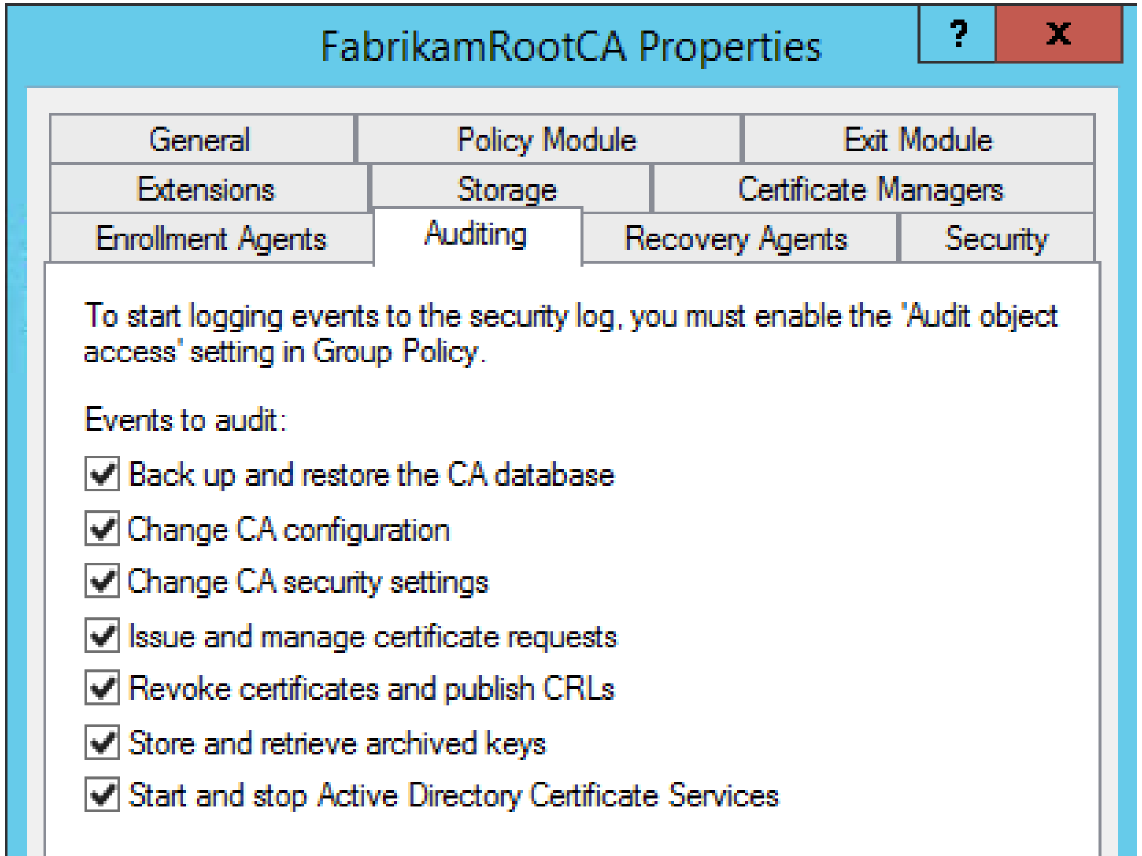
Value:

```
[1]Locations
     Distribution Point Name:
          Full Name:
URL=ldap:///CN=FabrikamRootCA,CN=FabrikamCorporatePKI,CN
=CDP,CN=Public Key
Services,CN=Services,CN=Configuration,DC=fabrikam,DC=com?
certificateRevocationList?base?objectClass=cRLDistributionPoint
(ldap:///CN=FabrikamRootCA,CN=FabrikamCorporatePKI,CN=CD
```

CA Auditing

Enabling auditing on the CA:

- Using certutil: **Certutil -setreg CA\AuditFilter 127**
- Using the GUI as described in the screenshot



FabrikamRootCA Properties

To start logging events to the security log, you must enable the 'Audit object access' setting in Group Policy.

Events to audit:

☑ Back up and restore the CA database

☑ Change CA configuration

☑ Change CA security settings

☑ Issue and manage certificate requests

☑ Revoke certificates and publish CRLs

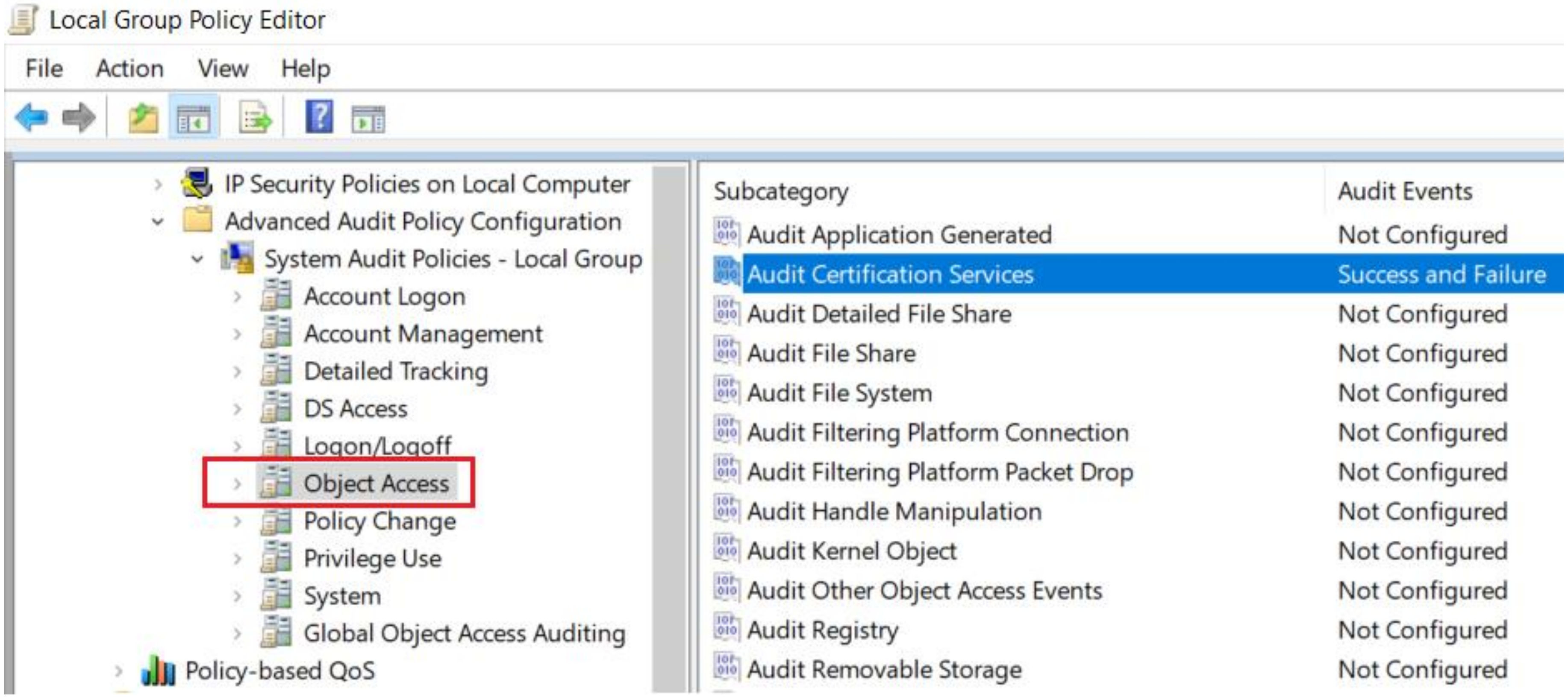
☑ Store and retrieve archived keys

☑ Start and stop Active Directory Certificate Services

CA Auditing (Cont.)

Enable auditing on the OS using Group Policy:

- Advanced Audit Policy Configuration > System Audit Policies > Object Access > Audit Certification Services


Local Group Policy Editor
File
Action
View
Help
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS

Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Success and Failure
Audit Detailed File Share	Not Configured
Audit File Share	Not Configured
Audit File System	Not Configured
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Not Configured
Audit Removable Storage	Not Configured

Lesson Review

Question 1:

How to enable Audit for Certificate Services?

The audit should be enabled for both the CA and the OS level.

Question 2:

What is the advantage of configuring the “Include in all CRLs” option at the offline root CA?

Simplify the process of manually publishing the Root CA CRL.

Lab

Module 4, Lab 2 Exercise 1:

Install and Configure Standalone Offline Root CA

Duration: 30 Minutes

Subordinate Issuing CA

Publishing Root CA certificate and CRL

As a prerequisite to the subordinate CA deployment, the Root CA certificate and CRL should be published to relevant locations.

1. Copy Root CA's CRT and CRL files to a domain-joined server
2. Publish Root CA certificate and CRL to Active Directory:
   - To the AIA and *Certification Authorities* containers: certutil -f –dspublish <RootCACertFileName.crt> RootCA
   - To the CDP container: certutil -f -dspublish FabrikamRootCA.crl FabrikamCorporatePKI
3. Publish Root CA certificate and CRL to the web server:
   - Copy the files to the relevant folder (CertData) under the web server
4. Update the subordinate local store with the new certificates:
   - gpupdate /force (on the subordinate CA server)

Install and Configure Subordinate Issuing CA

- Install AD CS role:
  - Member server running Windows Server 2016, fully patched with network connection and static IP
  - CA common name cannot be changed, domain membership status cannot be changed without uninstalling CA
  - Machine name can be changed during migration or when requested

Post-install Configuration

- Using a secure method (USB or external media), copy subordinate CA certificate request file to the root CA:
  - Submit a request to the Root CA using CA manager
  - Issue certificate on the Root CA
  - Export certificate as .p7b
  - Using USB or external media to move the .p7b file back to the subordinate CA
- Import certificate into subordinate CA
  - Install the CA certificate using CA manager (certsrv.msc)

Post-install Configuration (continued)

- Start the CA service
- Delete all published certificate templates using CA manager (not necessary if LoadDefaultTemplates=0 used in CAPolicy.inf)
- Define CRL publication intervals
- Define CDP and AIA URLs (change defaults to appropriate HTTP/LDAP URLs)
- Define Validity Period
- Configure CA auditing
- Configure object access auditing using local security policy
- Restart AD CS service
- Publish new CRL

Lab

Module 4, Lab 2 Exercise 2:

Install and configure the User Issuing CA (Subordinate CA)

Duration: 30 Minutes

PowerShell-based Installation of Subordinate Issuing CA

PowerShell 4.0 Deployment Cmdlets (ADCS)

- The following Cmdlet copies the binaries for the appropriate role to the system:
  - Add-WindowsFeature <Role> -IncludeManagementTools

- The <Role> parameter can be replaced with the following options:
  - Adcs-Device-Enrollment
  - Adcs-Web-Enrollment
  - Adcs-Enroll-Web-Svc
  - Adcs-Enroll-Web-Pol
  - Adcs-Online-Cert

PowerShell 4.0 Deployment Cmdlets (ADCS)

The following Cmdlet install/remove the appropriate role:

- Install-/Uninstall-<Role>

The <Role> parameter can be replaced with the following options:

- AdcsCertificationAuthority
- AdcsNetworkDeviceEnrollmentService
- AdcsWebEnrollment
- AdcsEnrollmentWebService
- AdcsEnrollmentPolicyWebService
- AdcsOnlineResponder

PowerShell 4.0 Deployment Cmdlets (ADCS)

Add- / Get- / Remove-

- CAAuthorityInformationAccess
  Configures Authority Information Access (AIA) or Online Certificate Status Protocol (OCSP) URI on a CA.
- CACrlDistributionPoint
  Configures certificate revocation list (CRL) distribution point uniform resource indicator (URI) where the CA publishes certification revocations.
- CATemplate:
  Configures certificate template to the CA.

Backup- / Restore- CARoleService

- Backs up/Restore the CA database and private key information.

Health Check Validation

- PKIView.msc (Enterprise PKI)
  - Verify status ‘**OK**’ for all items for each CA
- AD CS Best Practices Analyzer (BPA)
  - Server Manager, AD CS role, BPA
    - Eight compliance checks
- Enroll an end entity certificate
  - Export certificate and check status
    - Certutil.exe –URL <CertFileName.cer>

Lab

# Module 4, Lab 2 –
Exercise 3 (Potional):

PowerShell-based Installation of Subordinate Issuing CA

Validate PKI Deployment Health

Duration: 30 Minutes

Lab

Module 4, Lab 2 Exercise 4:

Validate PKI Deployment Health

Duration: 15 Minutes

Module Summary

- Installation and configuration of an offline Root CA
- Installation and configuration of a subordinate Issuing CA using GUI and PowerShell
- Design and configure CDP and AIA
- Understand the different containers under “Public Key Services” container in AD

Microsoft