TOPIC: DEPLOYING AND MANAGING AD CS

Objective:

To deploy and configure a two-tier certification authority (CA) hierarchy consisting of an offline root CA and an enterprise subordinate CA, and to publish the root CA certificate throughout the domain.

Pre-requisites:

- Active Directory Domain Services (AD DS) deployed and configured.
- Appropriate administrative privileges on the domain controllers and CA servers.
- Network connectivity among servers.
- VMware Workstation setup with these virtual machines: LON-DC1 (Domain Controller), LON-SVR1 (Subordinate CA server), CA-SVR1 (Offline Root CA server).
- Lab environment domain: RPSLAB.COM (adapt as needed).
- Passwords and credentials for domain administrators (e.g., Pa$$w0rd).

Procedure:

Exercise 1: Deploying an Offline Root CA

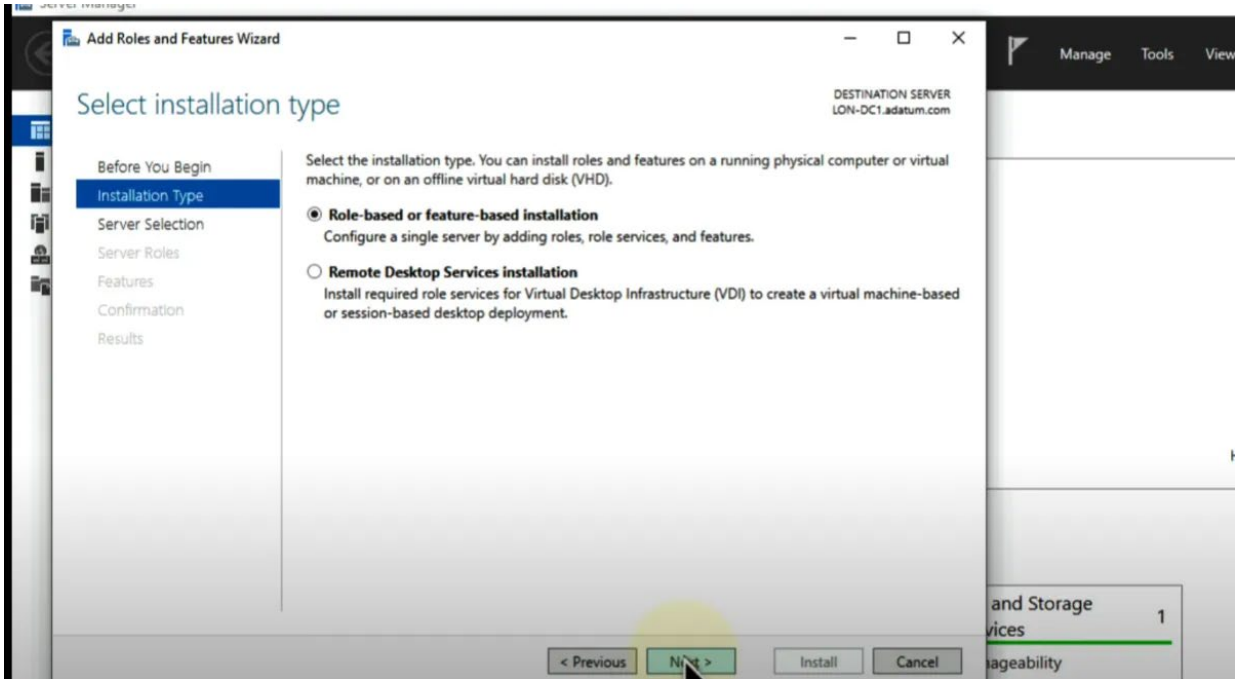
1. **Configure File and Printer Sharing Exceptions**
    - On CA-SVR1 and LON-SVR1, enable file and printer sharing in network advanced sharing settings.
2. **Install and Configure Active Directory Certificate Services (AD CS) on CA-SVR1**
    - Use Server Manager to add the AD CS role.
    - During installation, select the Certification Authority role service.
    - Configure AD CS as a standalone root CA.
    - Create a new private key with 4096-bit key length.
    - Name the CA as "AdatumRootCA."

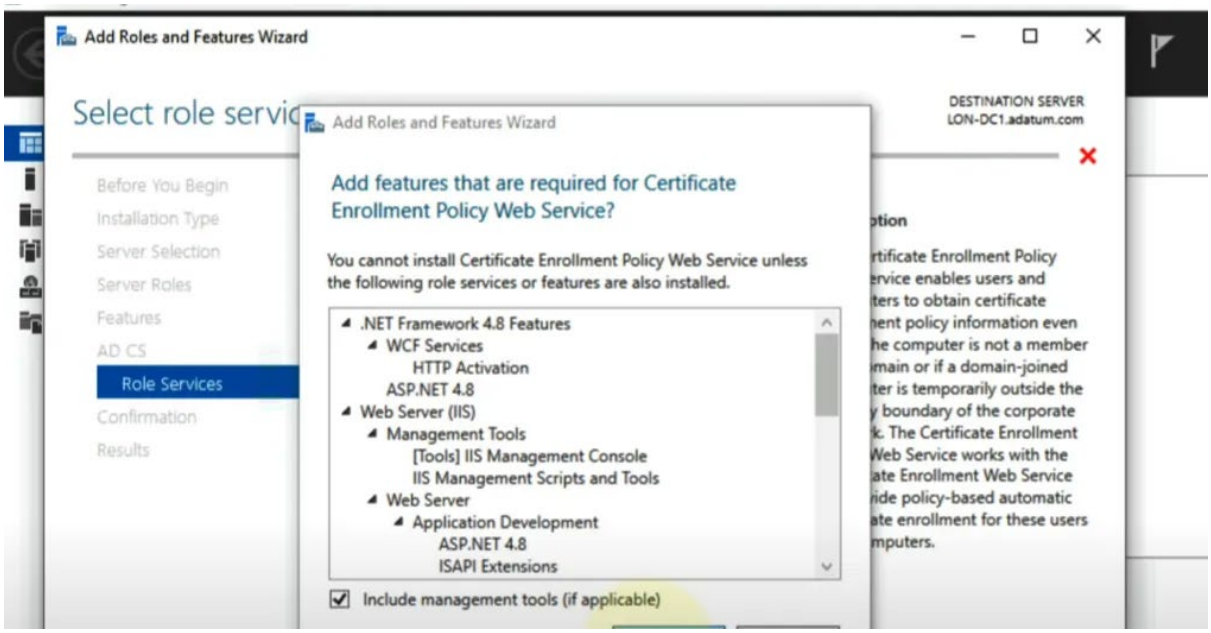
- Configure CRL Distribution Points (CDP) and Authority Information Access (AIA) with URLs pointing to http://lon-svr1.adatum.com/CertData/ with appropriate variables.
- Publish the Certificate Revocation List (CRL).
- Export the root CA certificate to a file RootCA.cer and copy it to a share accessible by the subordinate CA.

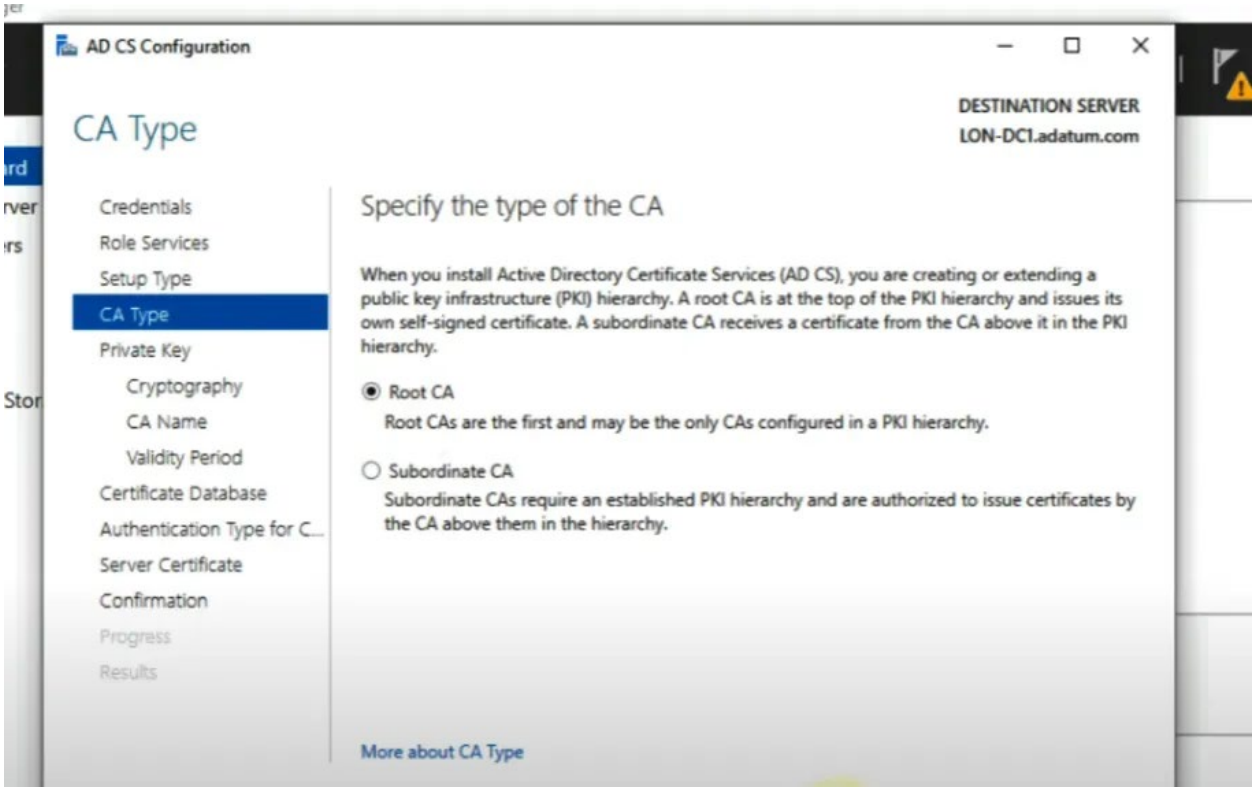
3. **Create a DNS Record for the Root CA**
    - On LON-DC1, add a new A (Host) DNS record for CA-SVR1 pointing to the root CA IP address 172.16.0.40.

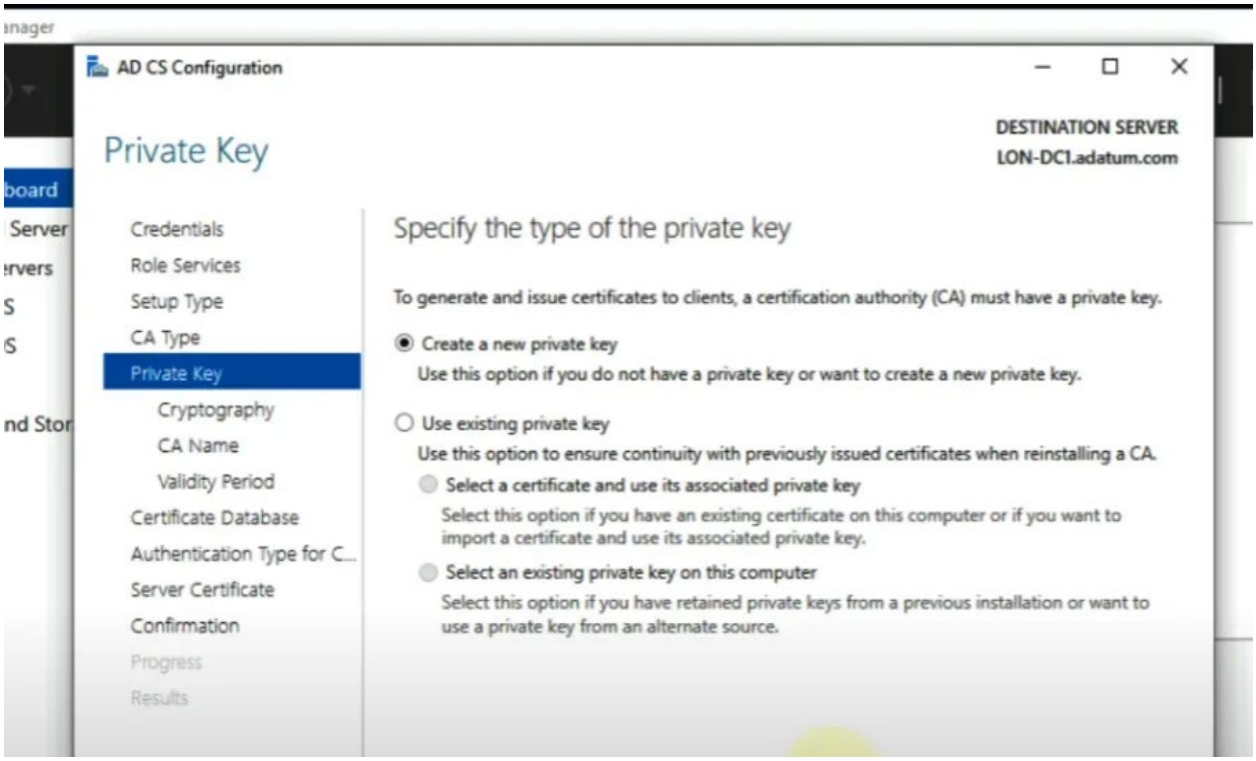
Exercise 2: Deploying an Enterprise Subordinate CA

1. **Install AD CS on LON-SVR1**
    - Add the AD CS role with Certification Authority and Certification Authority Web Enrollment services.
    - Configure as an enterprise subordinate CA.
    - Create a new private key.
    - Name the CA as "Adatum-IssuingCA".
    - Save certificate request to file.

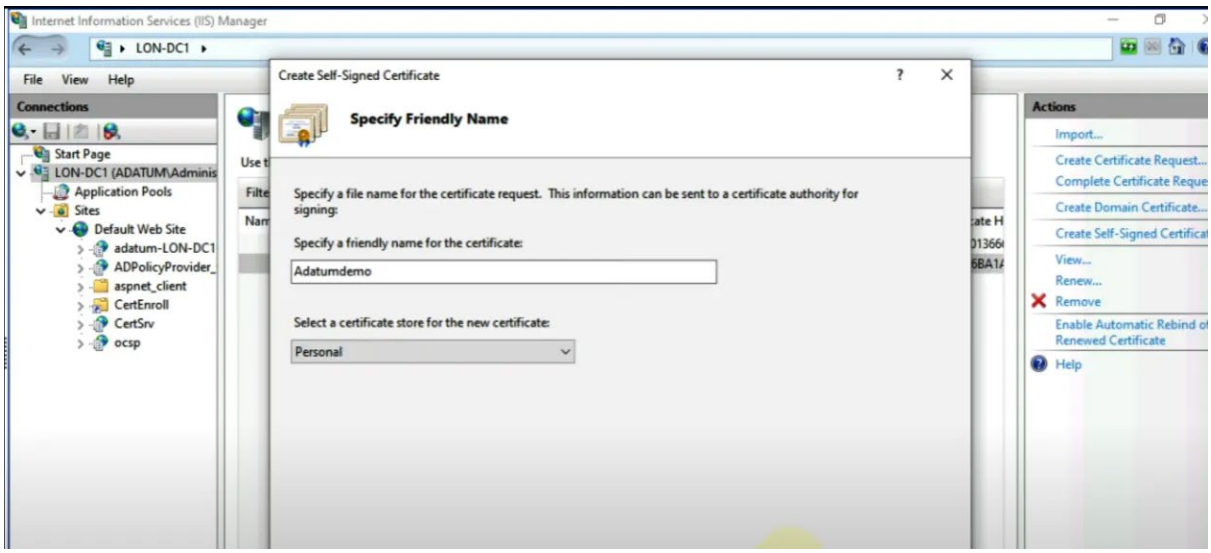


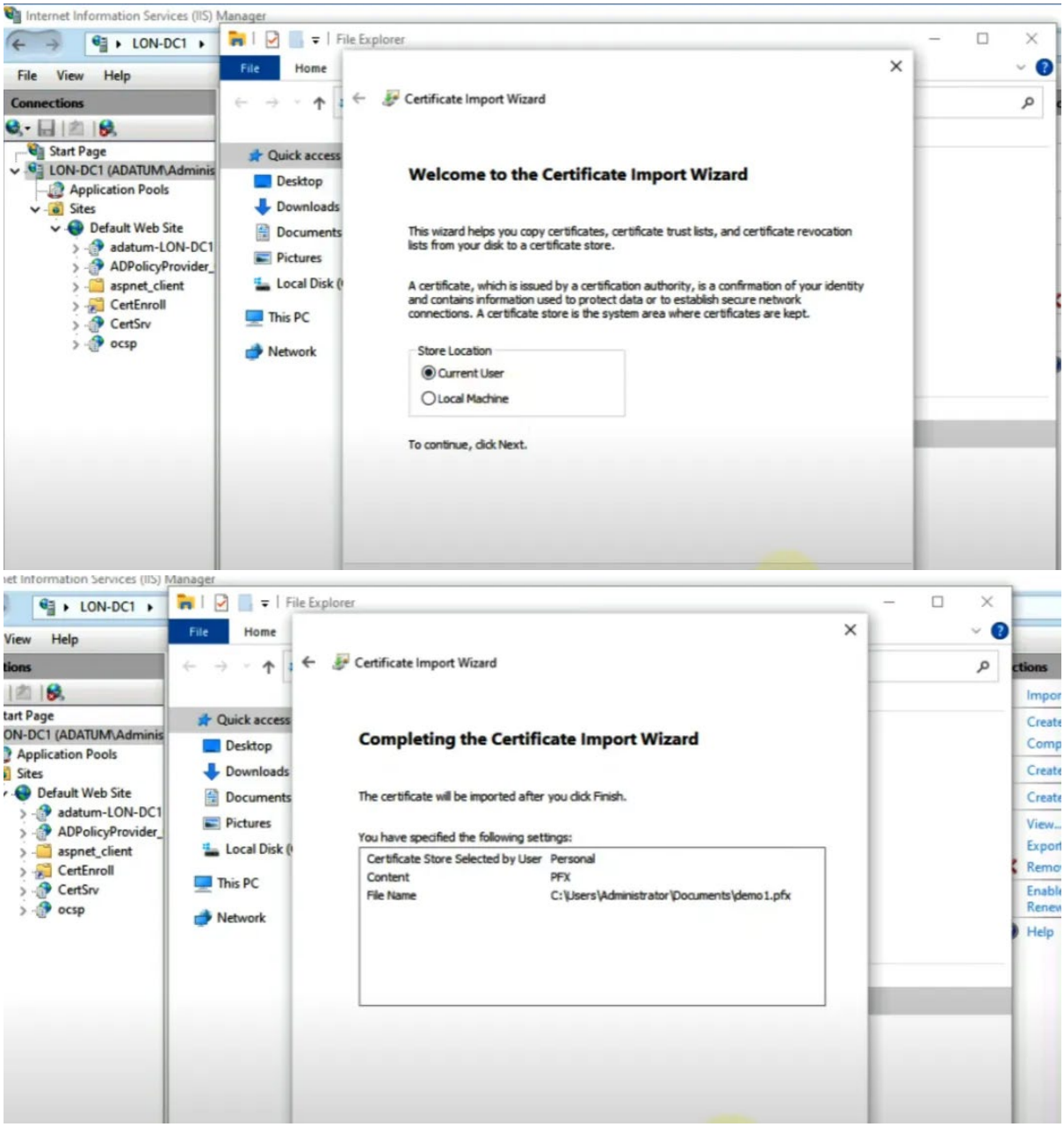

Add Roles and Features Wizard
Select role servic
DESTINATION SERVER
LON-DC1.adatum.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Certificate Enrollment Policy Web Service?
You cannot install Certificate Enrollment Policy Web Service unless the following role services or features are also installed.
.NET Framework 4.8 Features
WCF Services
HTTP Activation
ASP.NET 4.8
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
IIS Management Scripts and Tools
Web Server
Application Development
ASP.NET 4.8
ISAPI Extensions
Include management tools (if applicable)


AD CS Configuration
CA Type
DESTINATION SERVER
LON-DC1.adatum.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Specify the type of the CA
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.
Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.
More about CA Type



2. **Install the Subordinate CA Certificate**
    - Transfer the certificate request file to CA-SVR1.
    - Submit the request on the offline root CA.
    - Issue and export the subordinate CA certificate as a .p7b file.
    - Import the subordinate CA certificate on LON-SVR1 and start the CA service.





3. **Publish the Root CA Certificate using Group Policy**
    - Import the root CA certificate into the Trusted Root Certification Authorities store via Group Policy on the Default Domain Policy for the domain.

Conclusion:

By completing this module, you have successfully deployed a two-tier CA hierarchy with an offline root CA and an enterprise subordinate CA. You configured CRL distribution points and authority information access for certificate revocation and validation. The root CA certificate is published across the domain to enable trust for certificates issued

by the subordinate CA. This hierarchical CA setup enhances security by keeping the root CA offline while allowing the subordinate CA to issue certificates to users and devices within the domain.