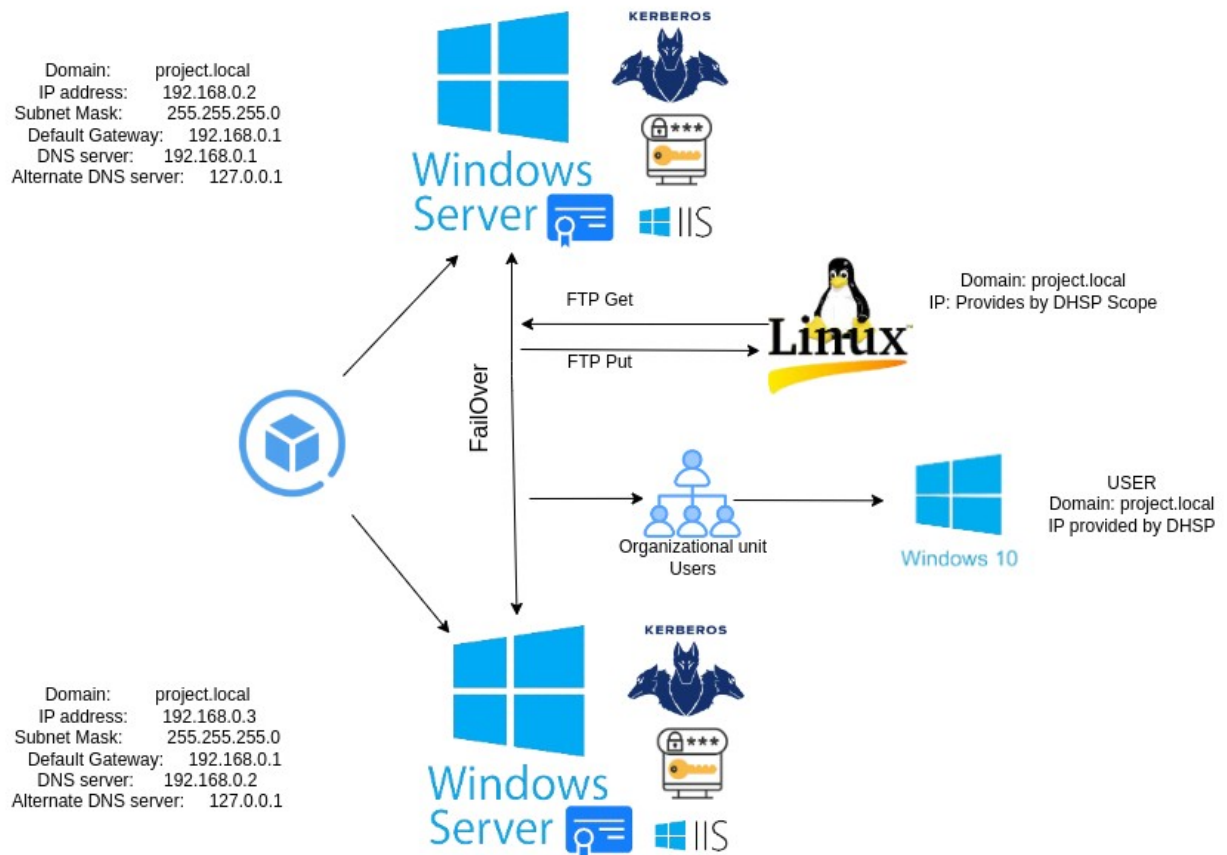


Windows server AD diagram



Secure Active Directory Setup for New Office

This project is about Windows Server Active Directory and we will configure it and understand how it works.

What is Active Directory?

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It allows administrators to manage permissions and control access to network resources by storing data as objects, including users, groups, applications, and devices, categorized according to their name and attributes. AD acts as a centralized location for managing users, computers, and other resources such as groups. Before Microsoft introduced the concept of a domain in Windows NT, user accounts were stored on individual PCs. AD allows for the storage of user accounts in a centralized location, where they can be easily managed by an administrator. It is a cornerstone of the modern enterprise IT infrastructure and serves as an essential tool for organizing and managing users, their attributes and group membership, computer accounts, network resources, and much more.

At first we need to install Virtual Box or VMware and Microsoft service ISO file

Virtual Box - <https://www.virtualbox.org/wiki/Downloads>

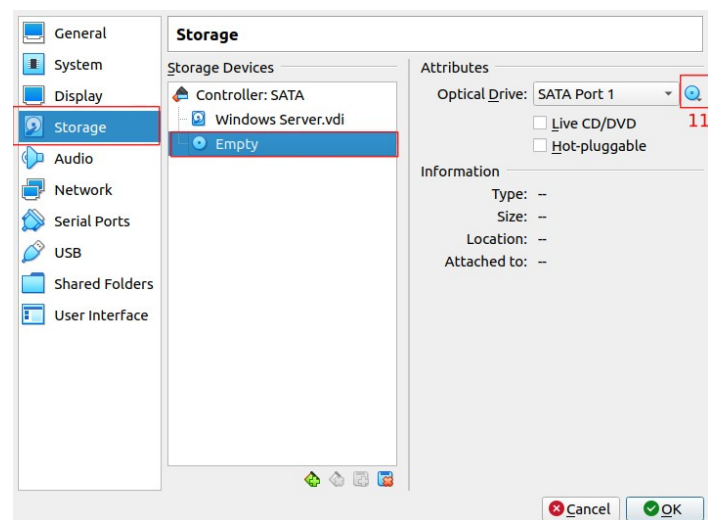
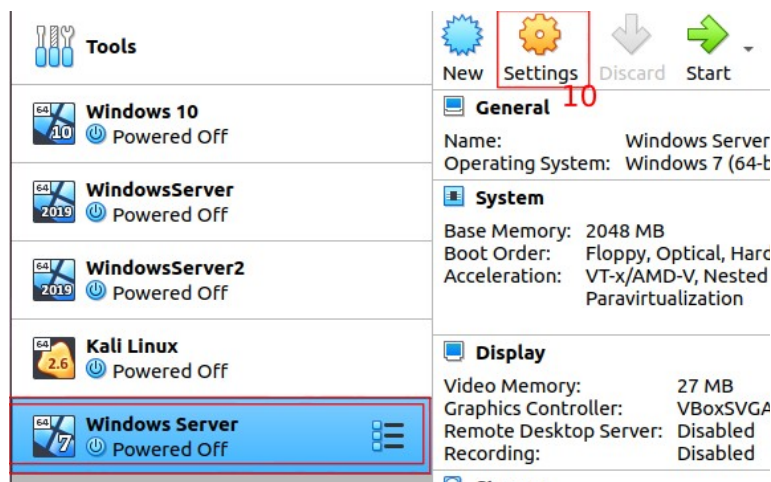
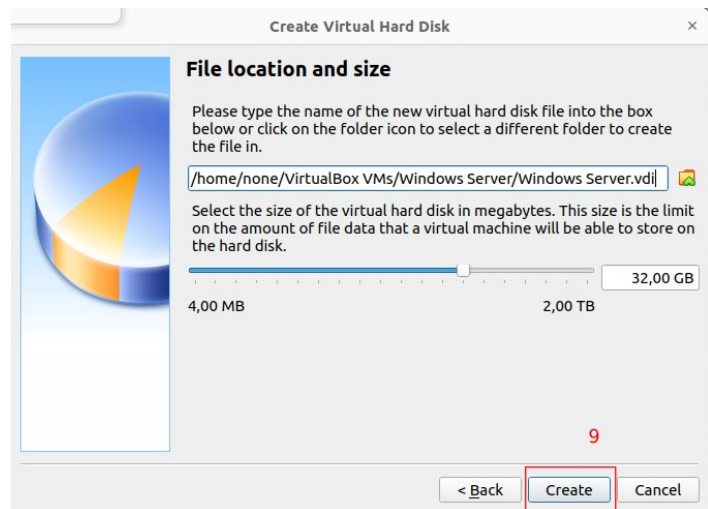
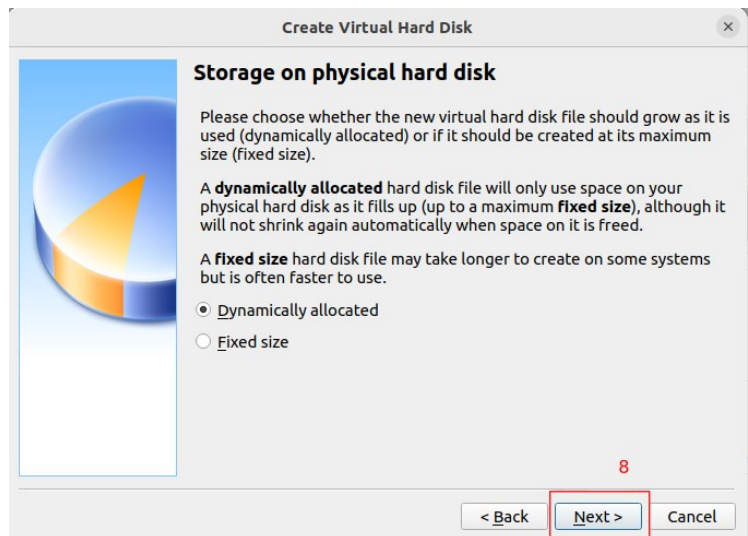
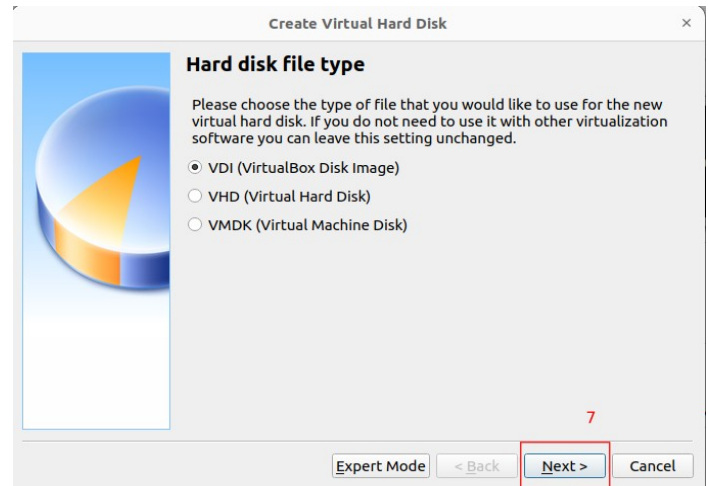
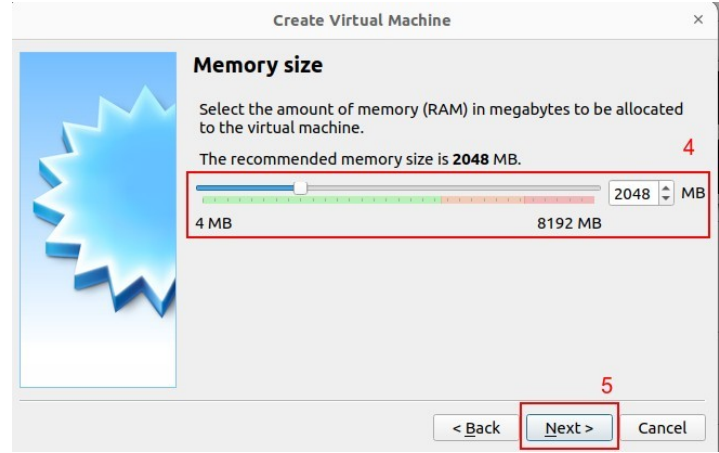
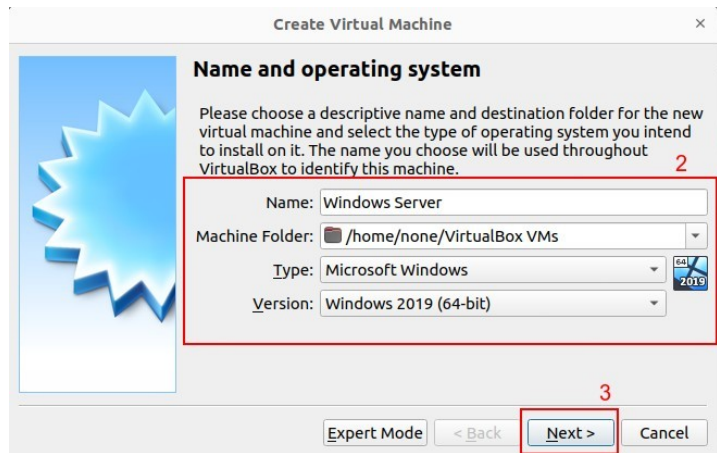
VMware - <https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html>

Microsoft service - <https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019>

After installation Virtual box install Microsoft service and setup it.

1. Select New





2. Write name, path, type and version and click next.
4. Select memory size (RAM) and click next.
6. click create
7. Select hard disk file type and click next.
8. Select storage type and click next.
9. Select .vdi file location and storage size and click create.
10. Open settings/storage/ select empty and put your ISO file there 11

After that start the machine and setup Windows server.

After installation you would see.

Create you administrator password and log in.

Select Add roles and featuers and install Active Directoery Domain Services, DHCP and DNS.

What is DHCP?

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically assign IP addresses and other communication parameters to devices connected to a network using a client-server architecture. It eliminates the need for manually configuring network devices and consists of two network components: a centrally installed network DHCP server and client instances of the protocol stack on each computer or device. DHCP automates and centrally manages these configurations, allowing devices to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. When a device wants access to a network using DHCP, it sends a request for an IP address that is picked up by a DHCP server.

What is DNS?

DNS, or Domain Name System, is **a naming database that converts human-readable domain names into numeric IP addresses**, allowing web browsers to access other internet resources. It is a hierarchical and distributed naming system for computers, services, and other resources in the Internet or other Internet Protocol (IP) networks. Without DNS services, users would need to type something like 172.16.254.1 every time they want to go to a particular website. DNS servers make it possible for people to input normal words into their browsers, such as Facebook.com, without having to keep track of the IP address for every website.

After installation, configure DHCP and DNS. I will show to to configure DNS.

Select Add a new forest and write your new domain name like mydomain.local and click next.

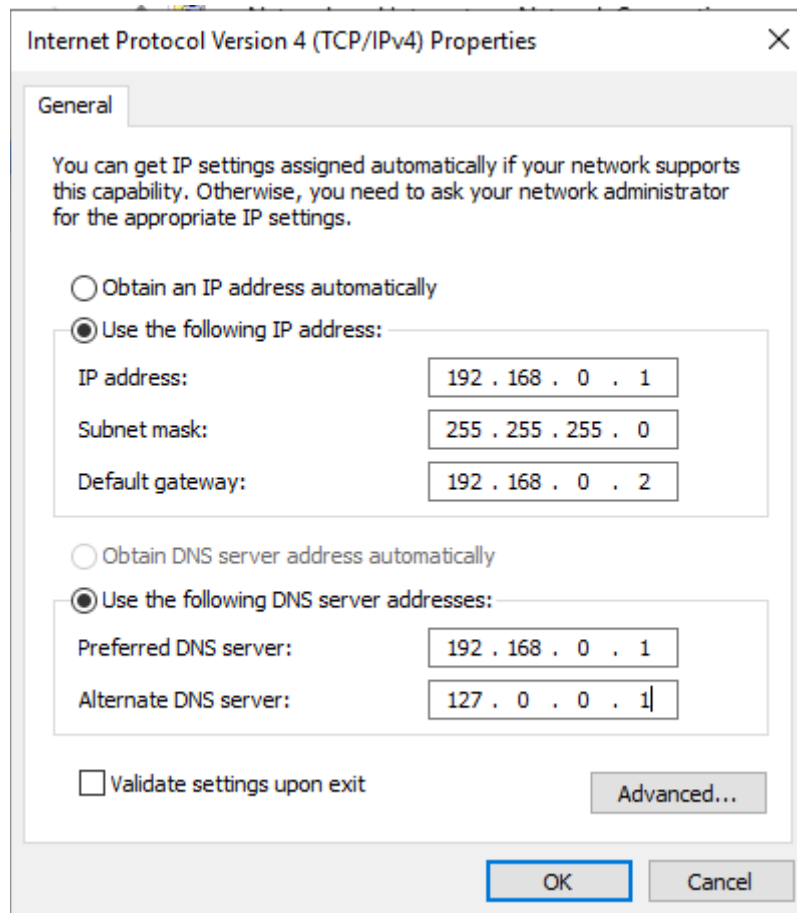
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the Windows logo and the text 'Active Directory Domain Services Configuration Wizard'. The window has a standard Windows interface with minimize, maximize, and close buttons. The main content area is titled 'Deployment Configuration'. On the left, there is a navigation pane with the following items: 'Deployment Configuration' (highlighted in blue), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area contains the following options: 'Select the deployment operation' with three radio buttons: 'Add a domain controller to an existing domain' (selected), 'Add a new domain to an existing forest', and 'Add a new forest'. Below this, 'Specify the domain information for this operation' includes a 'Domain:' text box and a 'Select...' button. Further down, 'Supply the credentials to perform this operation' shows '<No credentials provided>' and a 'Change...' button. At the bottom right, there is a link 'More about deployment configurations'. The bottom of the window features a grey bar with four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Create your password and click next.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Domain Controller Options' screen. The title bar and window controls are the same as the previous screenshot. The navigation pane on the left now has 'Domain Controller Options' highlighted in blue. The main content area is titled 'Domain Controller Options'. It includes the following settings: 'Select functional level of the new forest and root domain' with two dropdown menus: 'Forest functional level:' set to 'Windows Server 2016' and 'Domain functional level:' set to 'Windows Server 2016'. Below these, 'Specify domain controller capabilities' has three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). The 'Type the Directory Services Restore Mode (DSRM) password' section has two text boxes: 'Password:' and 'Confirm password:'. At the bottom right, there is a link 'More about domain controller options'. The bottom of the window features a grey bar with four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

click next in all places, without change anything and click install.

Now. Let's setup **IP** from Local Server select ethernet and in opened window press right-click on ethernet logo select properties and double click on ipv4 and write ip by you own. Like 192.168.0.1



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 0 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 2

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: 127 . 0 . 0 . 1

☐ Validate settings upon exit

Advanced...

OK Cancel

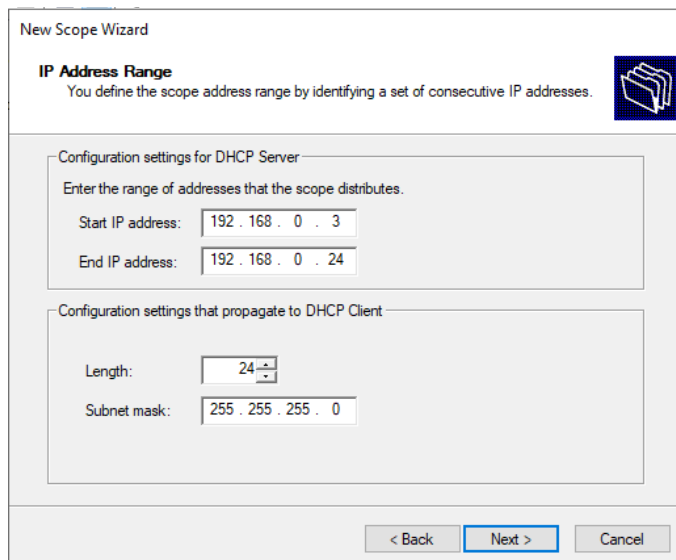
Now. Let's create user and give administrators permissions. From tools, select Active Directory user, and computers open your domain and press right-click on Users, and from new select user. Write your user name password and click create. After creation user double click on it and select member of give administrator permissions. You can see it in your administrator user permissions.

And now sign out of the administrator and log in to the user that was created.

After that you can disable administrator account.

Create scope. From tools select DHCP open IPv4 right-click on IPv4 select new scope

write your scope name and click next
write you IP range and click next



New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

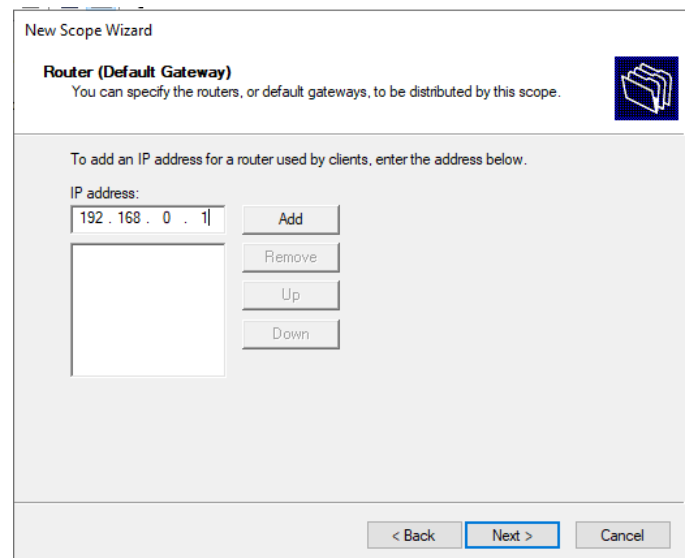
Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 0 . 3
End IP address: 192 . 168 . 0 . 24

Configuration settings that propagate to DHCP Client

Length: 24
Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel



New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address: 192 . 168 . 0 . 1
Add
Remove
Up
Down

< Back Next > Cancel

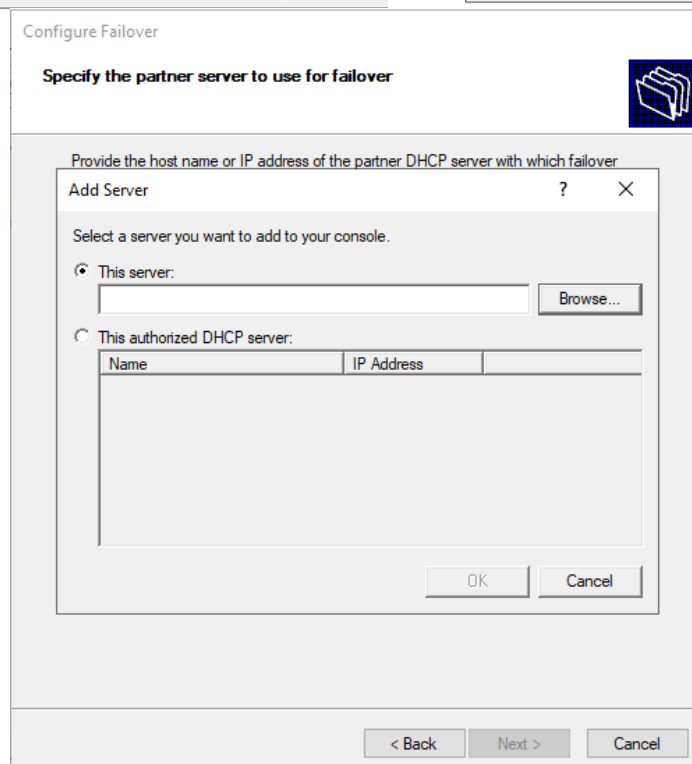
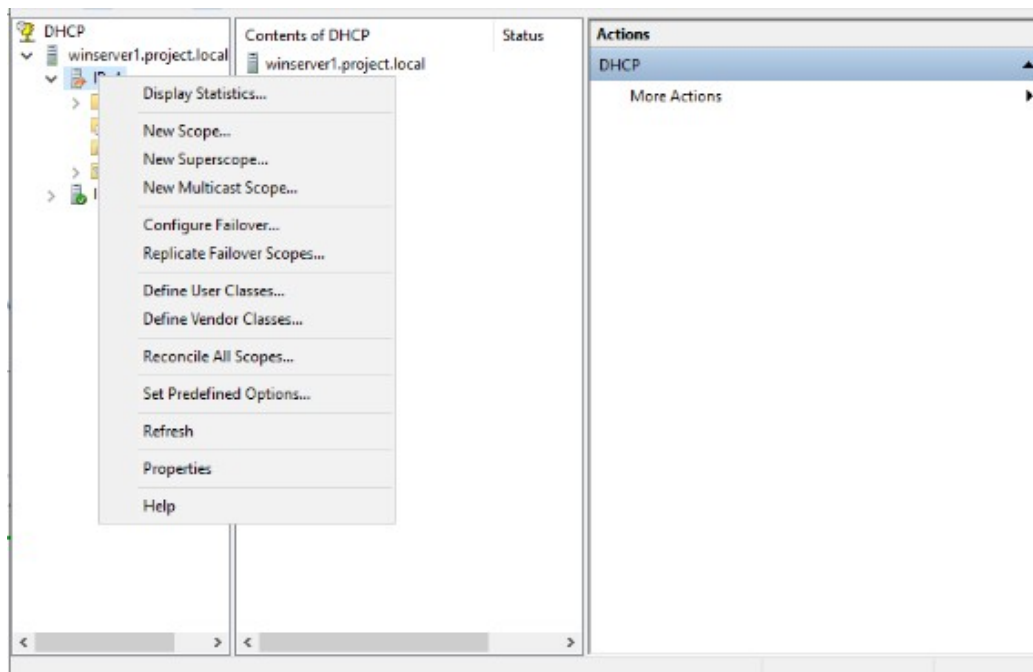
Failover (load balancing)

What is load balancing?

Load balancing is **a technique used to distribute network traffic evenly across multiple servers to improve application responsiveness, increase availability, and reduce latency.** It is a core networking solution that distributes network traffic across multiple servers in a server farm. A load balancer is a device that sits between the user and the server group and acts as an invisible facilitator, ensuring that all resource servers are used equally. By spreading the work evenly, load balancing improves application responsiveness and increases the availability of applications and websites for users. Load balancing can optimize the response time and avoid unevenly overloading some compute nodes while other compute nodes are left idle.

For installation load balancing, you need to set up a second server connected to the first server's domain.

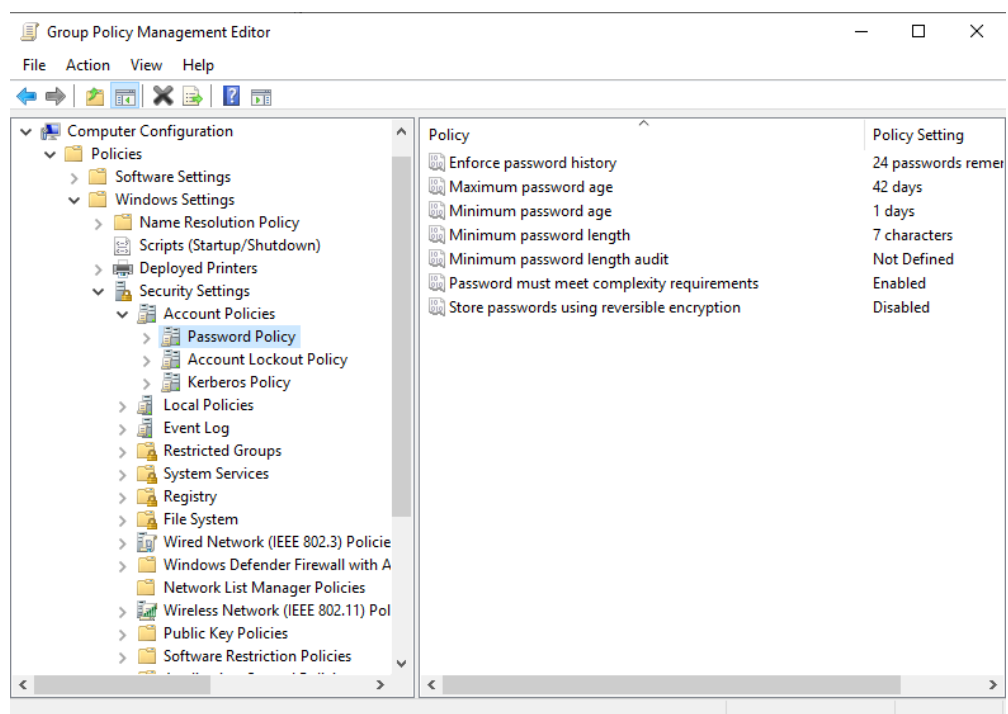
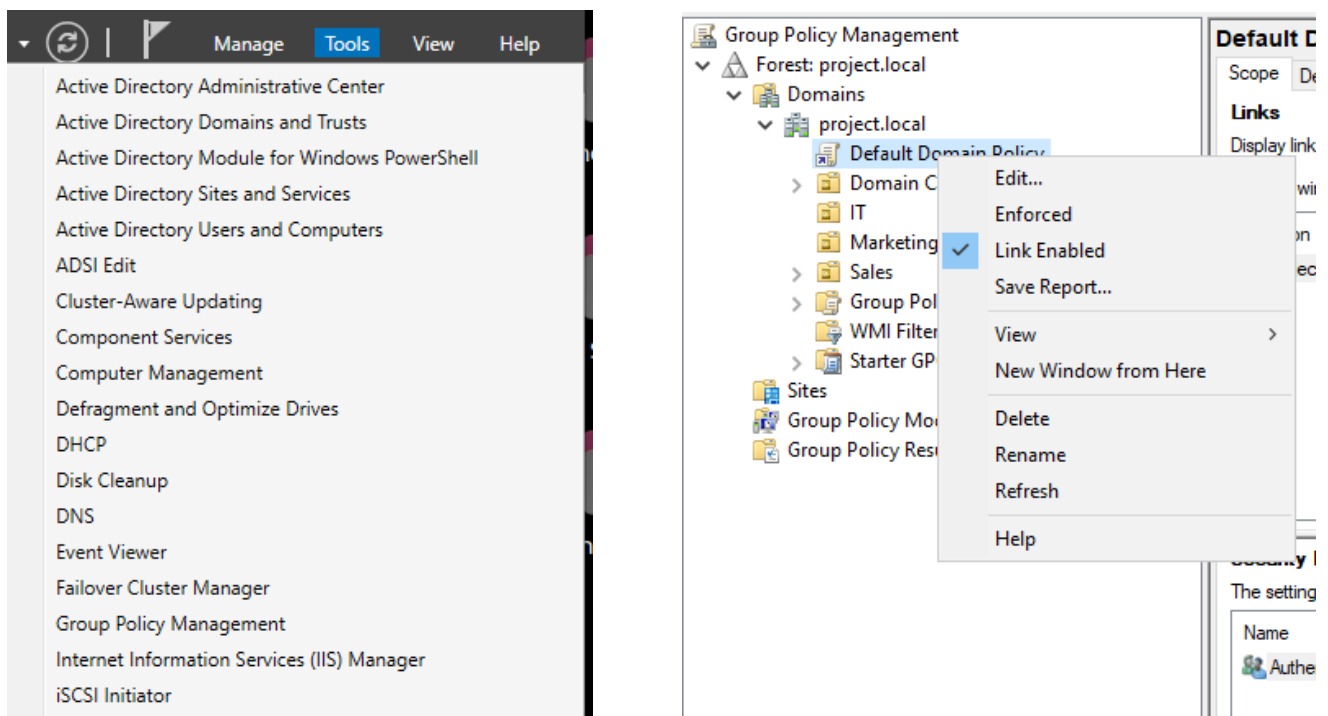
From tools select DHCP open right-click on IPv4 and select configure failover



click next, add server and select you second server IP click OK, next and write settings.

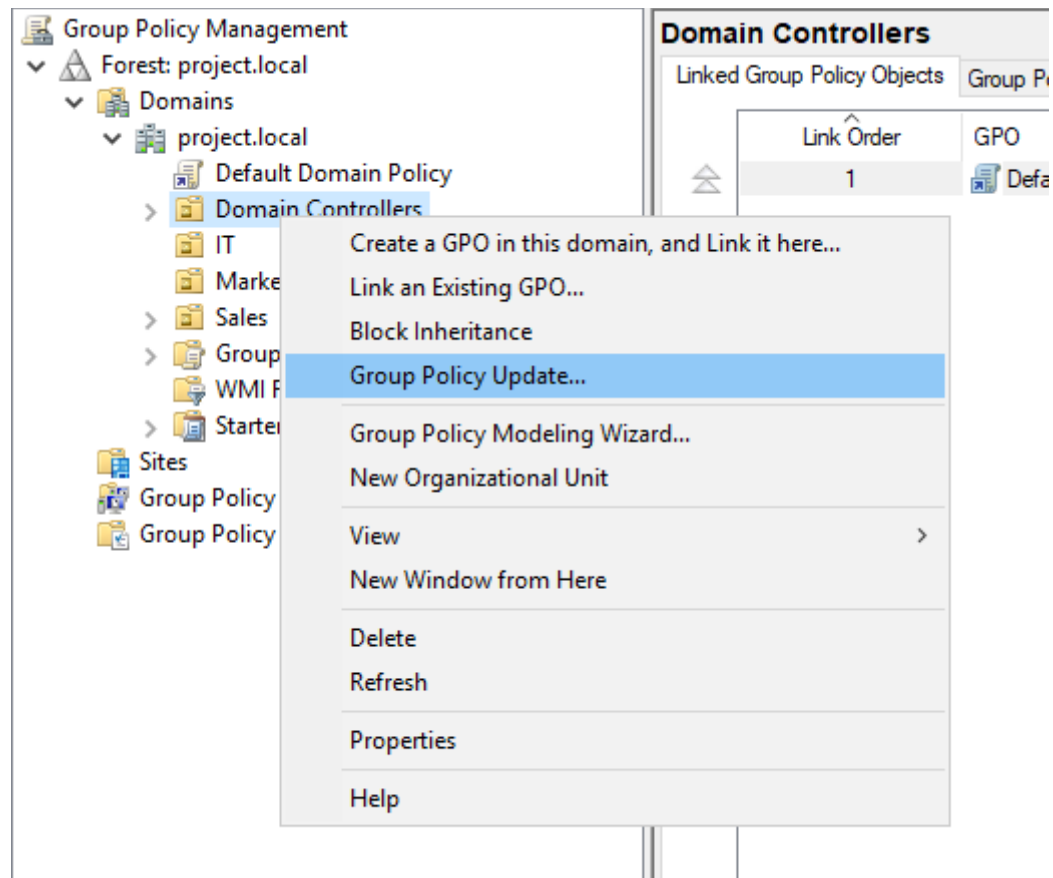
Password Policy

A password policy is **a set of rules designed to enhance computer security by encouraging users to create and implement stronger passwords**. It is a part of an organization's official regulations and is often included in security awareness training. Password policies can include requirements related to the length and complexity of the password, the expiration period, password reuse, and disallowing known breached passwords. An effective password policy is a set of rules that govern password creation and prevent sensitive data from being stolen. Even low-risk points of access can have a massive impact on a business if it falls into the wrong hands.



Now. Let's change the password policy. From tools, select Group Policy Management.

open forest:project.local/Domains/ right-click Default Domain Policy and click Edit, and then open Policies/Windows Settings/Security Settings/Account Policy and open Password Policy. Here you can make your changes, and then open Account Lockout Policy, and if you want, you can make changes or save default settings. After that, you need to update policies.



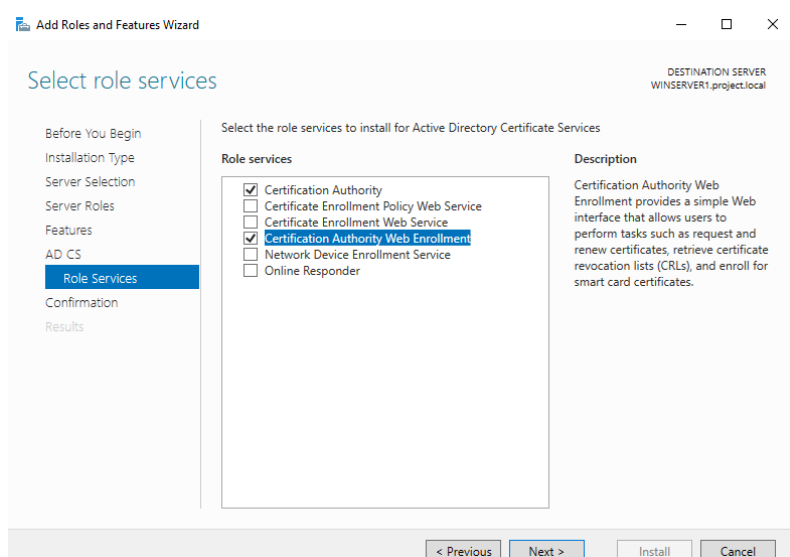
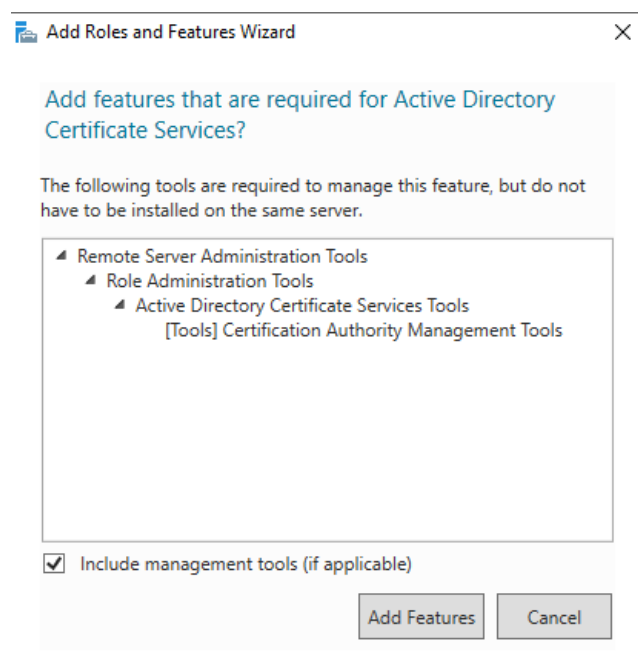
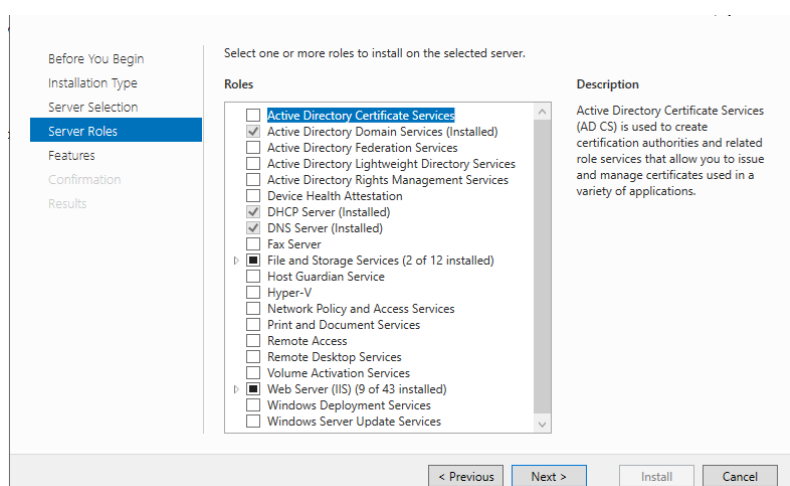
From group policy management, right-click on Domain Controllers and click on Group Policy Update, or in CMD, write gpupdate/force.

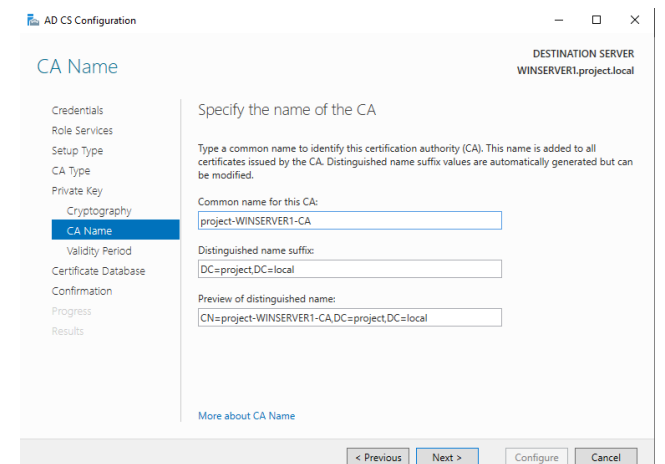
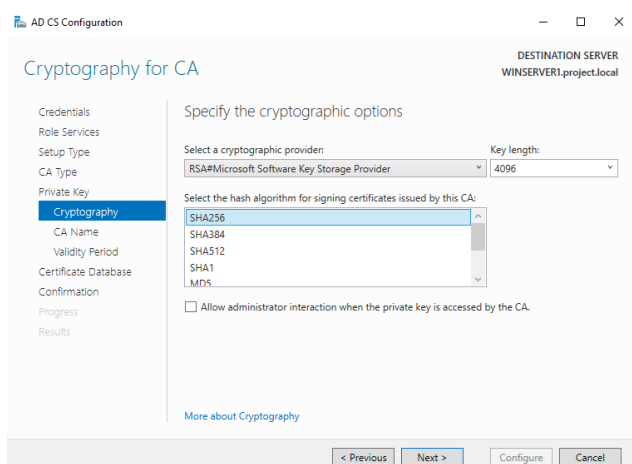
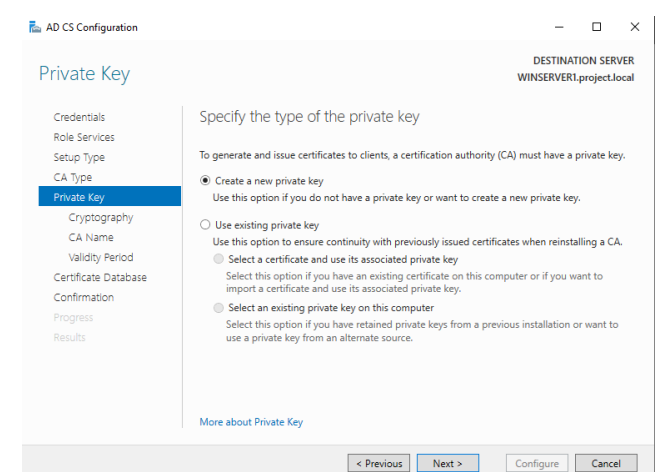
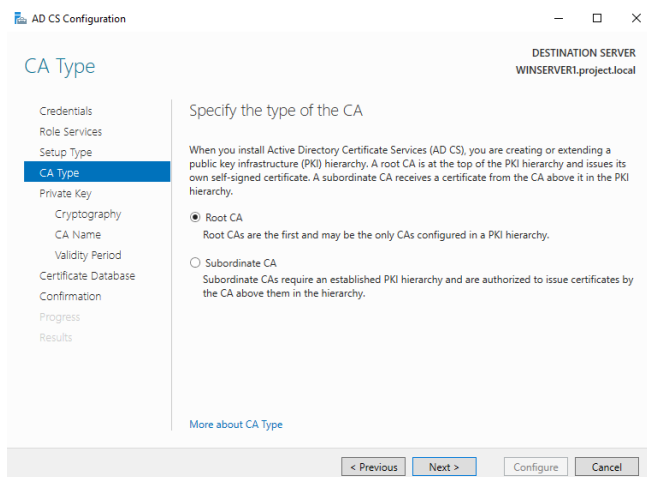
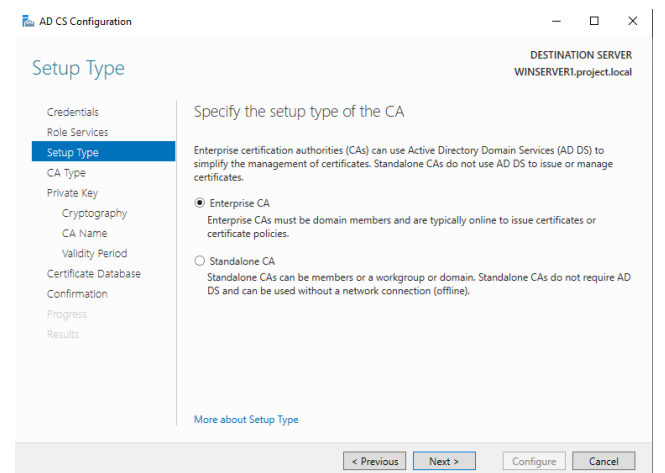
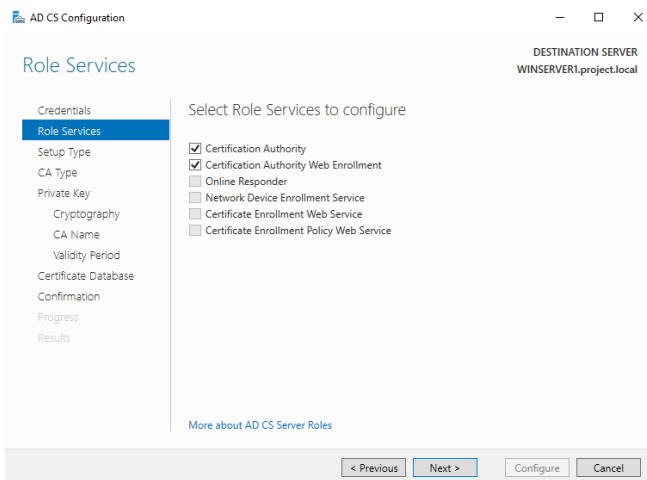
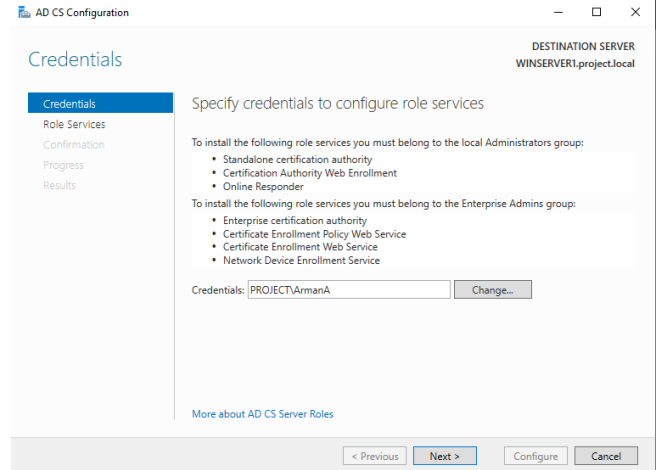
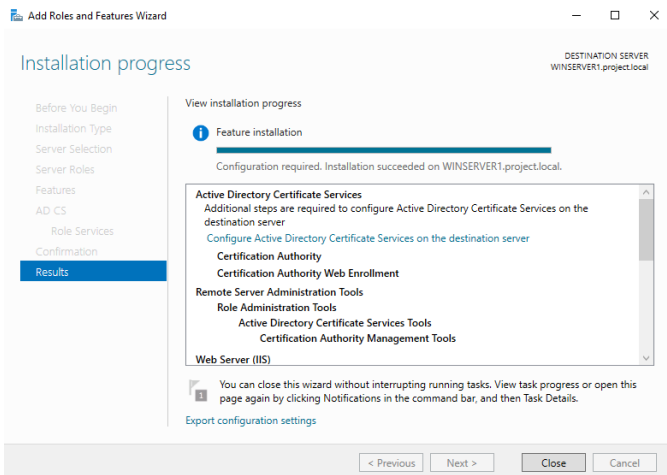
Active Directory Certificate Services

Active Directory Certificate Services (AD CS) is a server role introduced in **Windows Server 2008** that provides customizable services for issuing and managing digital certificates used in software security systems that employ public key technologies. It creates, approves, and rejects public key endorsements for inward tasks of an association and provides public key cryptography, digital certificates, and digital signature capabilities for an organization. AD CS is used to secure communication, verify the identity of users and devices, and facilitate secure data exchange in a network. However, AD CS has become a prime target and leverage point in the overall attack chain to achieve post-compromise objectives, making it challenging for cyber defenders to manage.

Now. Let's install and configure AD Certificate Services

2 Add roles and features





AD CS Configuration

DESTINATION SERVER
WINSERVER1.project.local

Validity Period

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 20.03.2029 15:22:00

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

< Previous Next > Configure Cancel

AD CS Configuration

DESTINATION SERVER
WINSERVER1.project.local

CA Database

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the database locations

Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

[More about CA Database](#)

< Previous Next > Configure Cancel

AD CS Configuration

DESTINATION SERVER
WINSERVER1.project.local

Confirmation

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type: Enterprise Root
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA256
Key Length: 4096
Allow Administrator Interaction: Disabled
Certificate Validity Period: 20.03.2029 15:22:00
Distinguished Name: CN=project-WINSERVER1-CA,DC=project,DC=local
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog

Certification Authority Web Enrollment

< Previous Next > Configure Cancel

Manage Tools View Help

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Module for Windows PowerShell
- Active Directory Sites and Services
- Active Directory Users and Computers
- ADSI Edit
- Certification Authority
- Cluster-Aware Updating
- Component Services
- Computer Management
- Defragment and Optimize Drives
- DHCP
- Disk Cleanup
- DNS
- Event Viewer
- Failover Cluster Manager
- Group Policy Management
- Internet Information Services (IIS) Manager

certsrv - [Certification Authority (Local)\project-WINSERVER1-CA\Certificate Templates]

File Action View Help

Certification Authority (Local)
project-WINSERVER1-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates

Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, CL...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypted...

http://localhost/certsrv/

Microsoft Active Directory Certificate Services -- project-WINSERVER1-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Click Add roles & features. Select Active Directory Certificate Services from Role Services, add Certification Authority and Certification Authority Web Enrollment, and install it. After installation, click Configure Active Directory Certificate Services on the destination server. From Role Services, add Certification Authority and Certification Authority Web Enrollment, click Next, select Enterprise CA, Next, select Root CA, and click Next. Create a new private key, enter the length of the key and hash algorithm, and from Confirmation, click Configure. From Tools, select Certification Authority, and there you can see all certifications. Your certification was added. Thank you.

FTP SERVER

File transfer protocol server (commonly known as FTP Server) is computer software that facilitates the secure exchange of files over a TCP/IP network. It runs the file transfer protocol (FTP), a standard communication protocol that operates at the network level, to establish a secure connection between the devices in a client-server architecture and efficiently transmit data over the internet.

FTP servers are the software solutions used for transferring files across the internet. They are primarily used for two essential functions, “Put” and “Get.” It allows uploading (Put) files to the server from the client device and downloading (Get) files from the server on the client device. FTP server helps to accommodate the following functions.

- **Exchange Large Size Files:** Organizations usually struggle to share large files over email. Businesses dealing with vast amounts of data often face interruptions during their file sharing process due to large files. The FTP server allows organizations to share large files without hassles.
- **Enhance Security:** The most significant purpose of employing FTP servers is to ensure a high level of security while sending sensitive data across the network. FTP servers also support other types of secure file transfer protocols such as SSH File Transfer Protocol (SFTP) and FTP Secure (FTPS) to add another layer of security. These protocols ensure effective end-to-end encryption to secure files while in transit.
- **Optimize Workflows:** FTP servers help enterprises streamline the file sharing process to overcome productivity challenges. With the right software application in place, users can share large volumes of data instead of sharing a single file at a time. Centrally storing files minimizes the time required to locate a file, and scheduled transfers help avoid any delays or interruptions across workflows.
- **Improve Control:** FTP servers empower businesses to exercise greater control over their data by providing smart access controls. Since every user requires different permissions to access various files, administrators can easily determine who can edit, upload, download, or share files based on permissions.
- **Reliable Disaster Recovery:** An effective FTP server ensures organizational data and files aren't compromised or lost in the wake of a disaster. Continuous and automatic backup helps in proactively storing data at other locations for easy restoration when needed.

How to Connect to SFTP Using FileZilla?

Download and Install FileZilla:

- Visit the official FileZilla website and download the appropriate version for your operating system (Windows, macOS, or Linux).

- Install FileZilla by following the installation prompts.

2. Open FileZilla and Enter Your FTP Credentials:

- Launch FileZilla after installation.

- You'll see the FileZilla interface with fields to enter your FTP login details:

- Host: Enter your website's domain or IP address (e.g., **ftp.example.com**).

- Username: Use the FTP username provided by your web host.

- Password: Enter the corresponding password.

- Port: Usually, the default FTP port is 21. If your host specifies a different port, enter it.

- Click the "Quickconnect" button to establish a connection.

3. Form the FTP Connection:

- Once connected, the left panel displays files on your local computer (your PC), and the right panel shows files on your remote server (your website).

- Navigate to the directories where you want to upload or download files.

4. Upload a File from Your Computer:

- In the left panel (local site), locate the file you want to upload.

- Drag and drop the file from the left panel to the right panel (remote site) to upload it to your website.

- Alternatively, right-click the file and choose "Upload."

5. Download a File from Your Website (Optional):

- To download a file from your website to your local computer:

- In the right panel (remote site), locate the file you want to download.

- Drag and drop it to the left panel (local site) or right-click and choose "Download."

