Lab Report: PKI with IIS (Windows)

Introduction

Public Key Infrastructure (PKI) is a framework of technology, policies, and procedures that enables the management of encryption keys and digital certificates. It is crucial for securing communications over unsecured networks like the Internet, ensuring the authenticity, integrity, and confidentiality of exchanged data.

1. Setting Up the Lab

Required Machines :

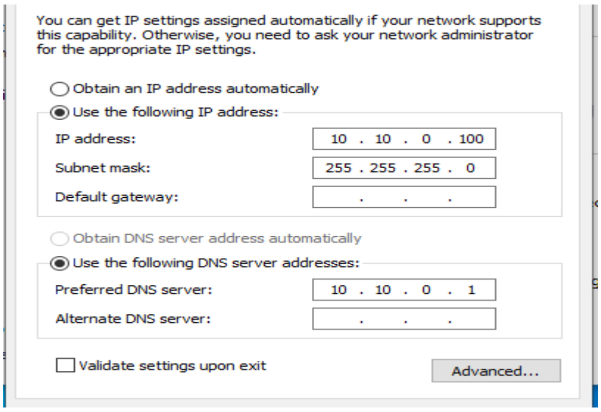
Windows 10 Client	Windows Server 2016 with IIS	Windows Server 2016 with AD DS, AD CS, DNS

2. Client Configuration

Log in as an administrator then Configure network settings according to the configuration table

IP Adresse	10.10.0.100
Hostname	client
DNS	10.10.0.1
Domaine	esi.dz

- Restart the machine and then create a standard user account: esi and log in with it.



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: 10 . 10 . 0 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 0 . 1
Alternate DNS server: . . .

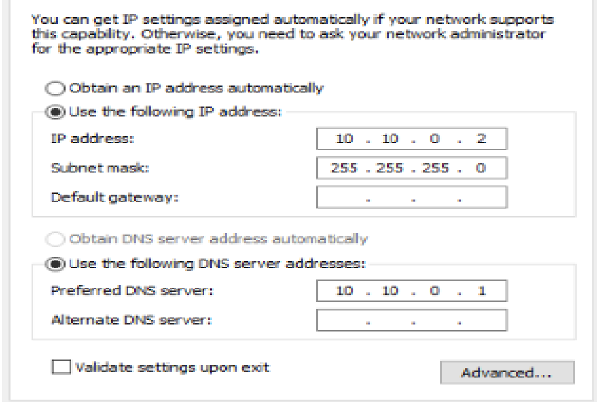
□ Validate settings upon exit

3. Web Server Configuration

- Virtual Machine Creation in VMware Workstation
- Create a new virtual machine with the following network settings:

Adresse IP	10.10.0.2
Hostname	Webserver
DNS	10.10.0.1
Domaine	esi.dz

- Restart the machine.



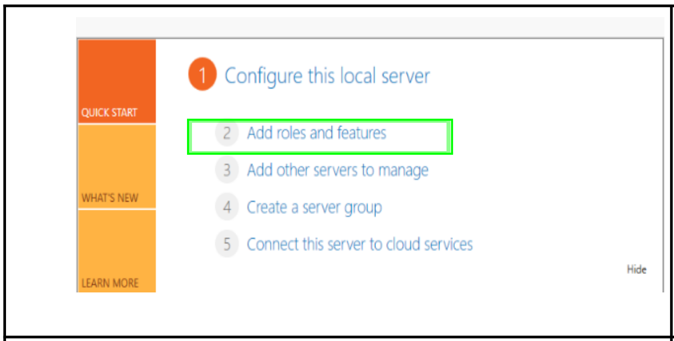
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

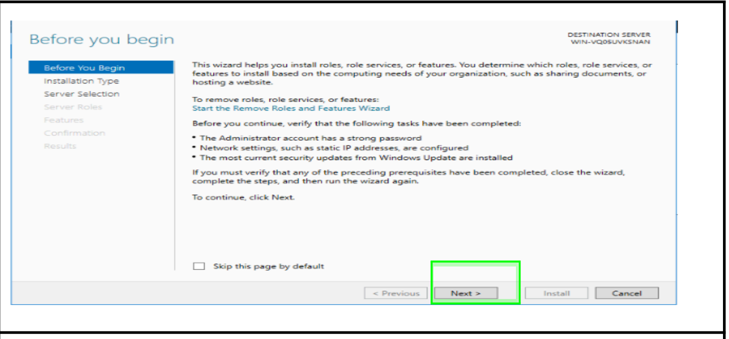
○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 10 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 0 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

1. **Install IIS :**
   - Open Server Manager and add the IIS role.


QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide


Before you begin

DESTINATION SERVER
WIN-VQ05UVKSNAN

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

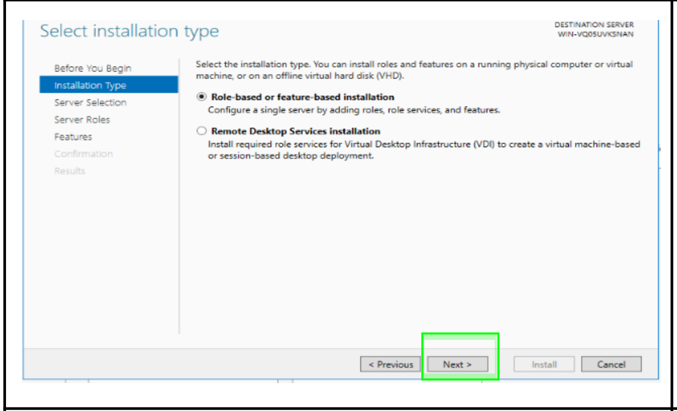
Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

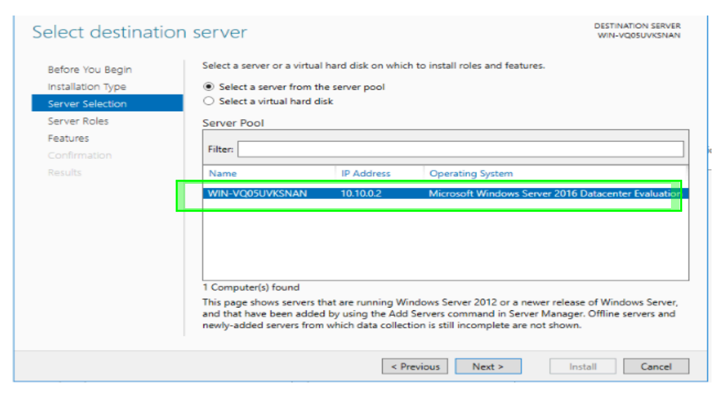

Select installation type

DESTINATION SERVER
WIN-VQ05UVKSNAN

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.


Select destination server

DESTINATION SERVER
WIN-VQ05UVKSNAN

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

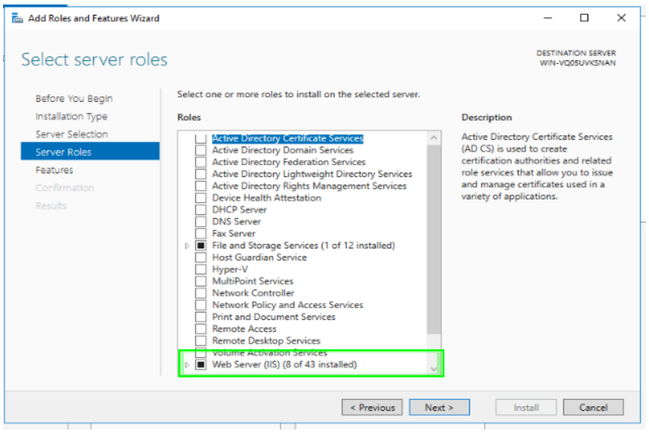
Server Pool

Filter:

Name	IP Address	Operating System
WIN-VQ05UVKSNAN	10.10.0.2	Microsoft Windows Server 2016 Datacenter Evaluation

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.


Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-VQ05UVKSNAN

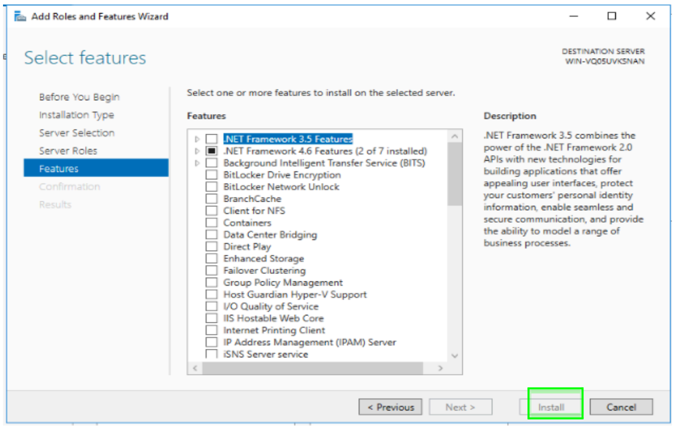
Select one or more roles to install on the selected server.

Roles

□ Active Directory Certificate Services
□ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Device Health Attestation
□ DHCP Server
□ DNS Server
□ Fax Server
■ File and Storage Services (1 of 12 installed)
□ Host Guardian Service
□ Hyper-V
□ MultiPoint Services
□ Network Controller
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
■ Web Server (IIS) (8 of 43 installed)

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.


Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-VQ05UVKSNAN

Select one or more features to install on the selected server.

Features

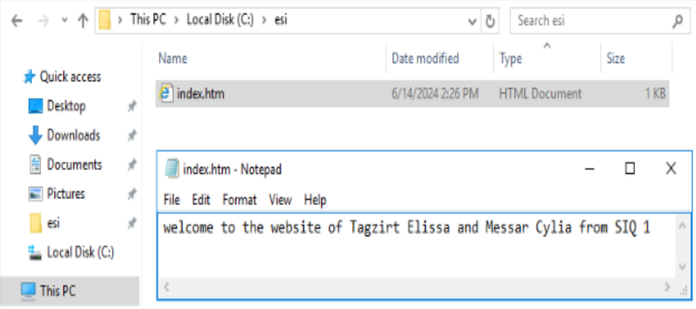
□ .NET Framework 3.5 Features
■ .NET Framework 4.6 Features (2 of 7 installed)
□ Background Intelligent Transfer Service (BITS)
□ BitLocker Drive Encryption
□ BitLocker Network Unlock
□ BranchCache
□ Client for NFS
□ Containers
□ Data Center Bridging
□ Direct Play
□ Enhanced Storage
□ Failover Clustering
□ Group Policy Management
□ Host Guardian Hyper-V Support
□ I/O Quality of Service
□ IIS Hostable Web Core
□ Internet Printing Client
□ IP Address Management (IPAM) Server
□ iSNS Server service

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

2. Website Creation :

- Create the site directory: D:\esi
- Add an index page: D:\esi\index.txt with the content: "Welcome to the website of Tagzirt Elissa and Messar Cylia from SIQ1", then rename it to index.htm.

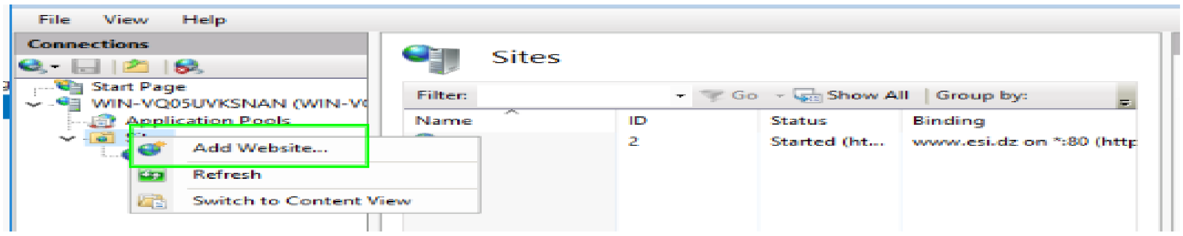

This PC › Local Disk (C:) › esi

Name	Date modified	Type	Size
index.htm	6/14/2024 2:26 PM	HTML Document	1 KB

```
welcome to the website of Tagzirt Elissa and Messar Cylia from SIQ 1
```

3. Configure IIS:

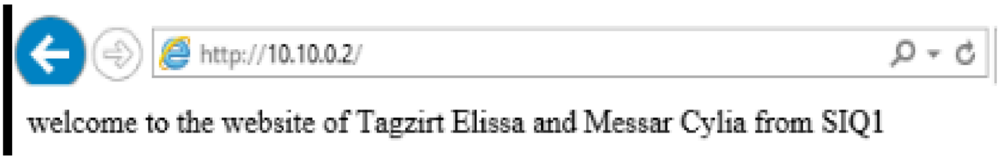
- Disable the default site.
- Add a new site named "esi" with the physical path D:\esi.



Name	ID	Status	Binding
	2	Started (ht...	www.esi.dz on *:80 (http

-

- Test the site at: http://10.10.0.2:80

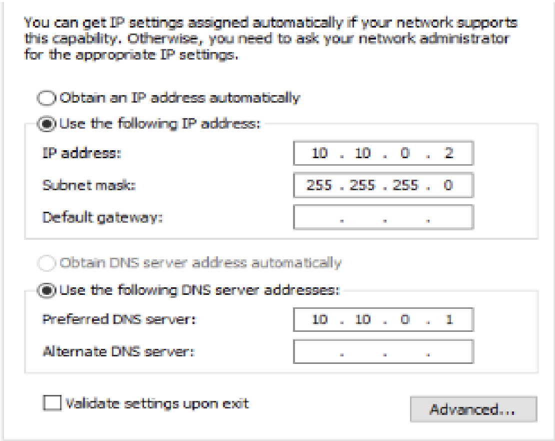

http://10.10.0.2/

welcome to the website of Tagzirt Elissa and Messar Cylia from SIQ1

4. DNS Configuration on the CA Machine

Create a new virtual machine with the following network settings:

IPAdresse	10.10.0.1
Hostname	CA
DNS	10.10.0.1
Domaine	esi.dz


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: 10 . 10 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

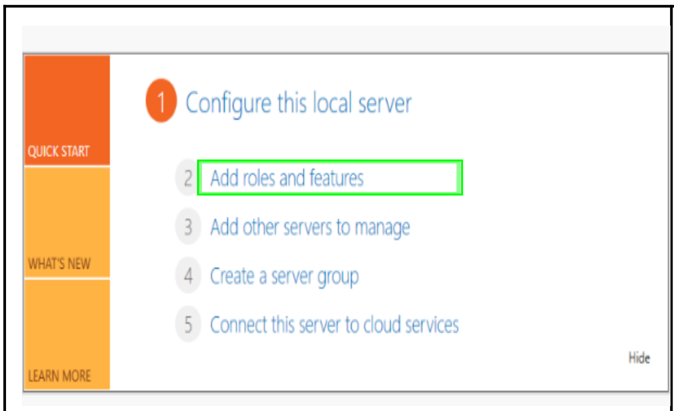
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 0 . 1
Alternate DNS server: . . .

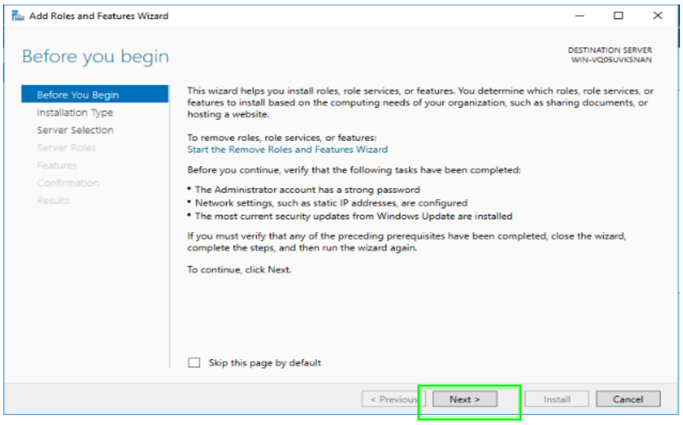
□ Validate settings upon exit

- Restart the machine.

1. Installation et configuration du rôle DNS sur la machine CA :

- Log in as an administrator.
- Open Server Manager and add the DNS role.


QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide



Before you begin

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

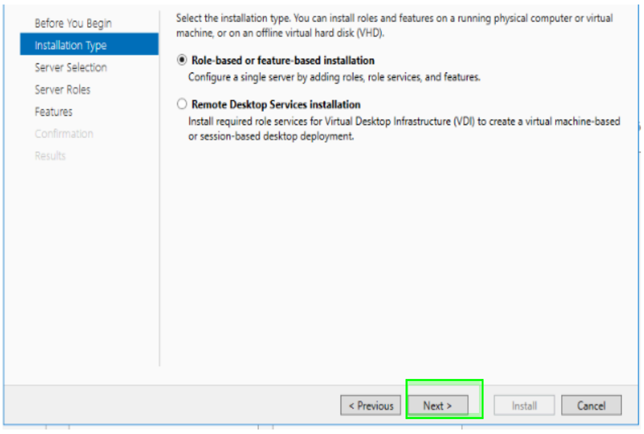
Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

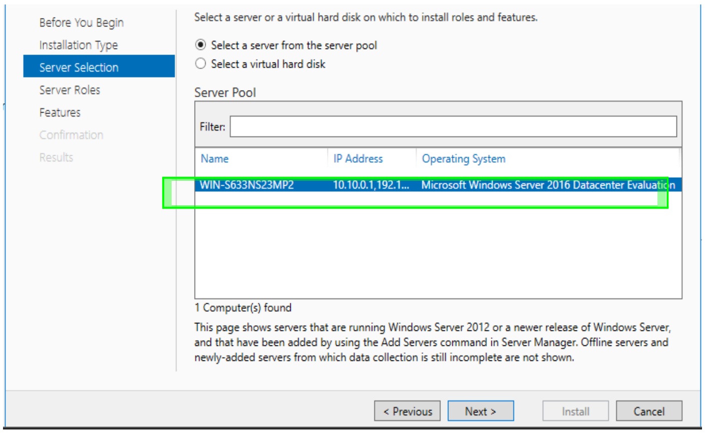
□ Skip this page by default



Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

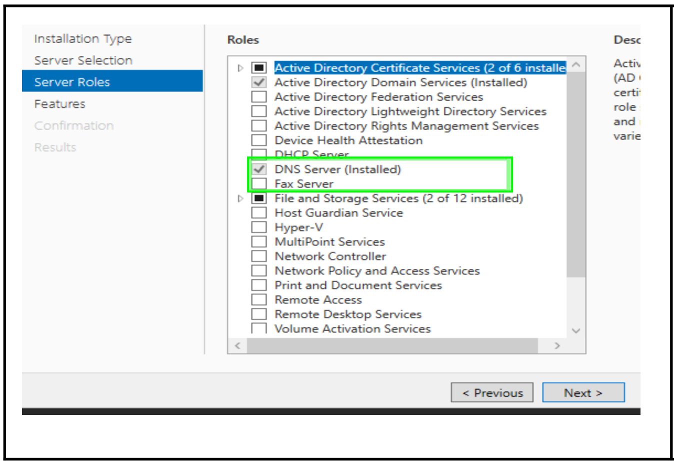
Server Pool

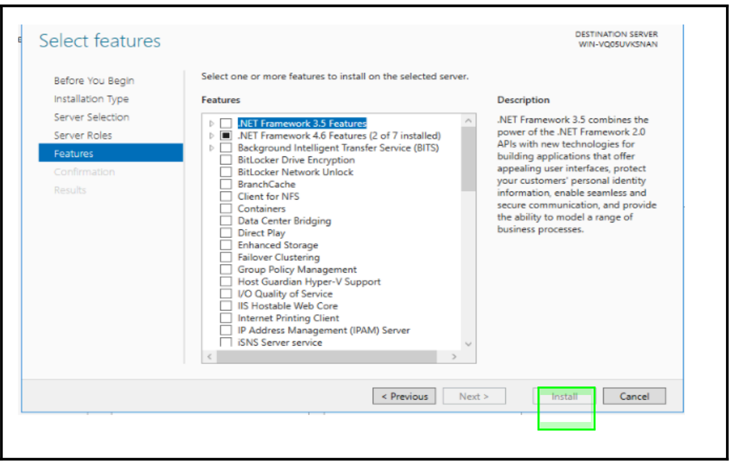
Filter:

Name	IP Address	Operating System
WIN-S633NS23MP2	10.10.0.1,192.1...	Microsoft Windows Server 2016 Datacenter Evaluation

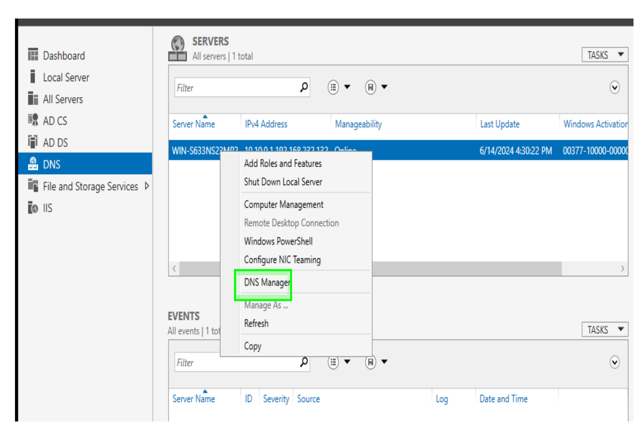
1 Computer(s) found

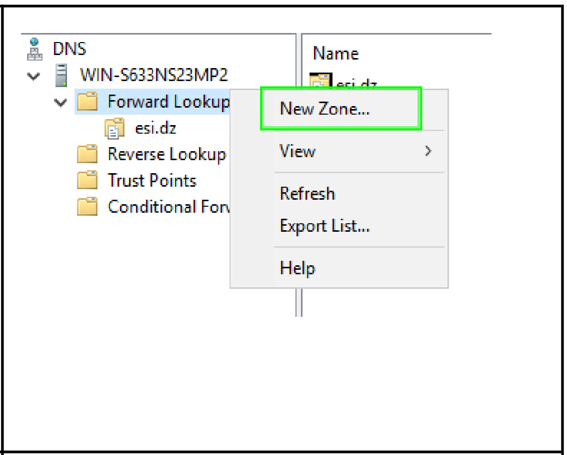
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

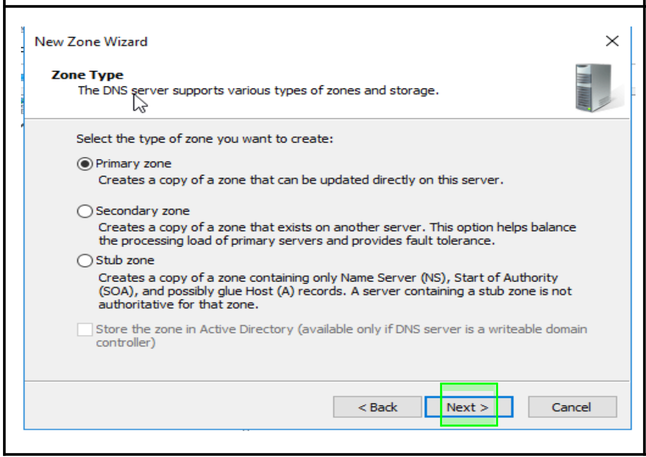

Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Roles
Desc
Active Directory Certificate Services (2 of 6 installe
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (2 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
< Previous
Next >


Select features
DESTINATION SERVER
WIN-VQ05UVKSNAN
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.6 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

- Open the DNS console.
- Add a new primary zone named: esi.dz.






New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

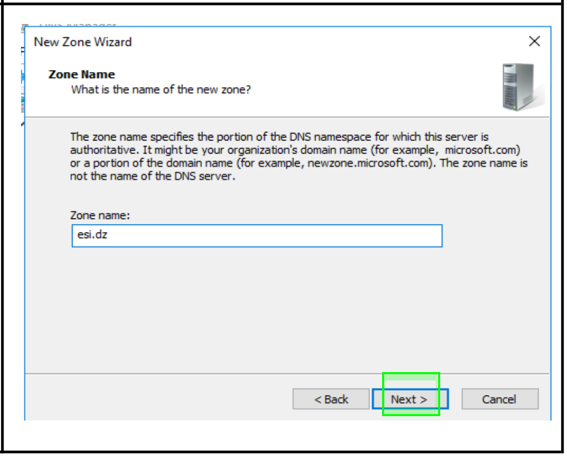
Select the type of zone you want to create:

● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

□ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)


New Zone Wizard

Zone Name
What is the name of the new zone?

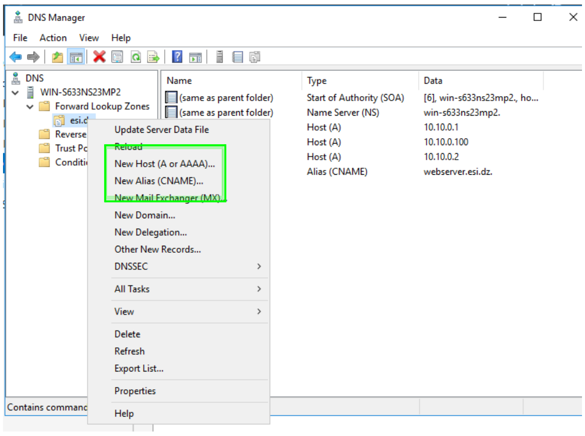
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:
esi.dz

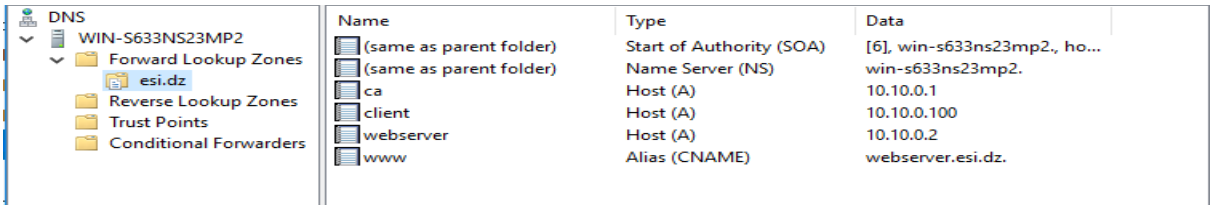
2. Adding DNS Records:

Add records to the primary zone esi.dz:

- www: CNAME record: webserver.esi.dz
- Client: A record: 10.10.0.100
- Webserver: A record: 10.10.0.2
- CA: A record: 10.10.0.1



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[6], win-s633ns23mp2., ho...
(same as parent folder)	Name Server (NS)	win-s633ns23mp2.
	Host (A)	10.10.0.1
	Host (A)	10.10.0.100
	Host (A)	10.10.0.2
	Alias (CNAME)	webserver.esi.dz.

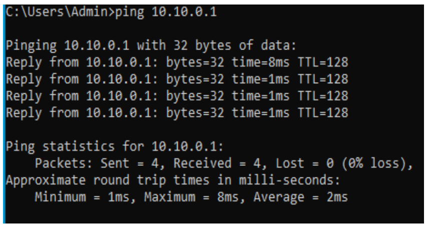
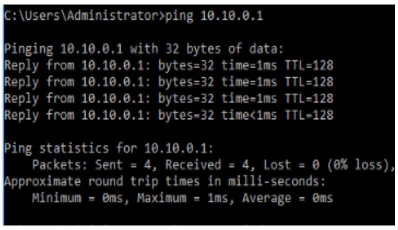
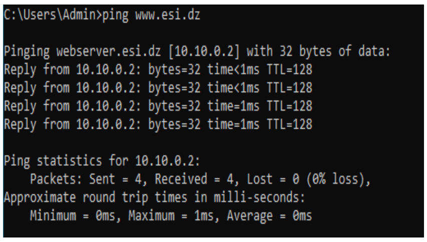
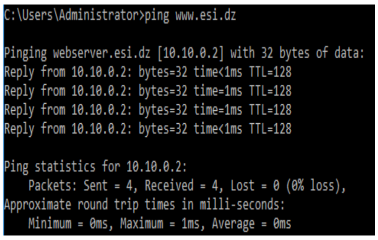
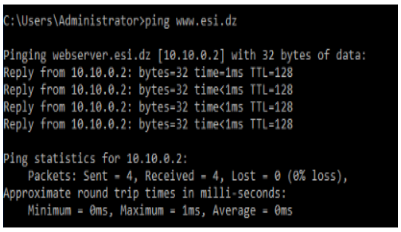


Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[6], win-s633ns23mp2., ho...
(same as parent folder)	Name Server (NS)	win-s633ns23mp2.
ca	Host (A)	10.10.0.1
client	Host (A)	10.10.0.100
webserver	Host (A)	10.10.0.2
www	Alias (CNAME)	webserver.esi.dz.

-

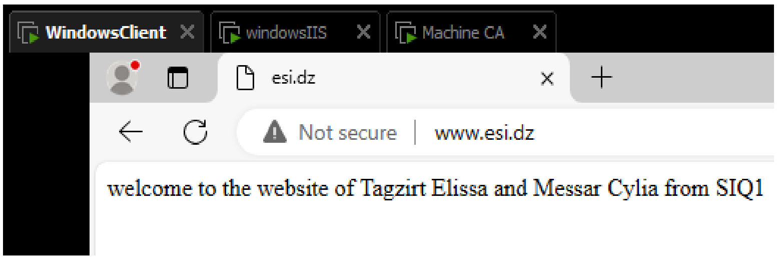
3. DNS Tests :

- On each machine, perform a ping to the other machines :

	client	CA	WebServer
ping 10.10.0.1	 C:\Users\Admin>ping 10.10.0.1 Pinging 10.10.0.1 with 32 bytes of data: Reply from 10.10.0.1: bytes=32 time=8ms TTL=128 Reply from 10.10.0.1: bytes=32 time=1ms TTL=128 Reply from 10.10.0.1: bytes=32 time=1ms TTL=128 Reply from 10.10.0.1: bytes=32 time=1ms TTL=128 Ping statistics for 10.10.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 8ms, Average = 2ms		 C:\Users\Administrator>ping 10.10.0.1 Pinging 10.10.0.1 with 32 bytes of data: Reply from 10.10.0.1: bytes=32 time=1ms TTL=128 Reply from 10.10.0.1: bytes=32 time=1ms TTL=128 Reply from 10.10.0.1: bytes=32 time=1ms TTL=128 Reply from 10.10.0.1: bytes=32 time<1ms TTL=128 Ping statistics for 10.10.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms
ping www.esi.dz	 C:\Users\Admin>ping www.esi.dz Pinging webserver.esi.dz [10.10.0.2] with 32 bytes of data: Reply from 10.10.0.2: bytes=32 time<1ms TTL=128 Reply from 10.10.0.2: bytes=32 time<1ms TTL=128 Reply from 10.10.0.2: bytes=32 time=1ms TTL=128 Reply from 10.10.0.2: bytes=32 time=1ms TTL=128 Ping statistics for 10.10.0.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms	 C:\Users\Administrator>ping www.esi.dz Pinging webserver.esi.dz [10.10.0.2] with 32 bytes of data: Reply from 10.10.0.2: bytes=32 time<1ms TTL=128 Reply from 10.10.0.2: bytes=32 time=1ms TTL=128 Reply from 10.10.0.2: bytes=32 time=1ms TTL=128 Reply from 10.10.0.2: bytes=32 time<1ms TTL=128 Ping statistics for 10.10.0.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms	 C:\Users\Administrator>ping www.esi.dz Pinging webserver.esi.dz [10.10.0.2] with 32 bytes of data: Reply from 10.10.0.2: bytes=32 time=1ms TTL=128 Reply from 10.10.0.2: bytes=32 time<1ms TTL=128 Reply from 10.10.0.2: bytes=32 time<1ms TTL=128 Reply from 10.10.0.2: bytes=32 time<1ms TTL=128 Ping statistics for 10.10.0.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

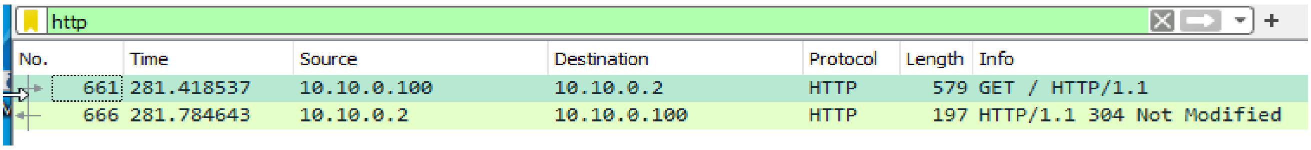
5. HTTP Tests

- On the client machine, open a web browser.
- Access the site at: http://www.esi.dz.



welcome to the website of Tagzirt Elissa and Messar Cylia from SIQ1

1. **Analyse avec Wireshark :**

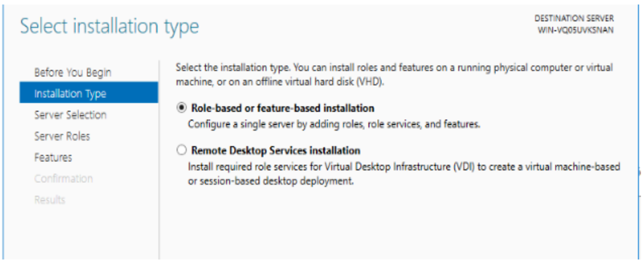


No.	Time	Source	Destination	Protocol	Length	Info
661	281.418537	10.10.0.100	10.10.0.2	HTTP	579	GET / HTTP/1.1
666	281.784643	10.10.0.2	10.10.0.100	HTTP	197	HTTP/1.1 304 Not Modified

6. Certificate Authority Configuration

1. Role Installation on the CA Machine

- Log in as an administrator.
- Add the AD DS and AD CS roles:
  - Open Server Manager.
  - Click on "Manage" then "Add Roles and Features".
  - Follow the wizard to install AD DS and AD CS roles.



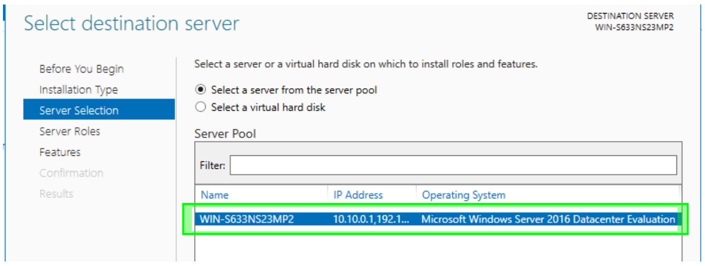
Select installation type

DESTINATION SERVER
WIN-VQ05UVKSNAN

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.

○ Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Select destination server

DESTINATION SERVER
WIN-S633NS23MP2

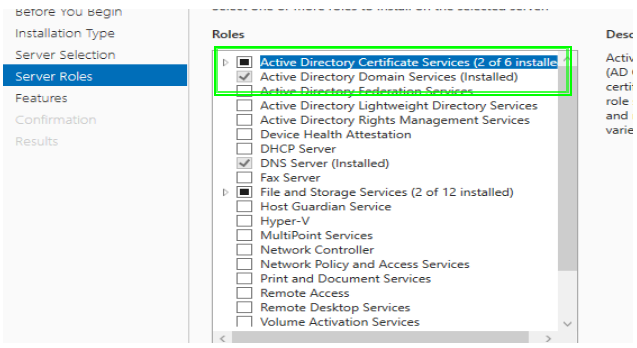
Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

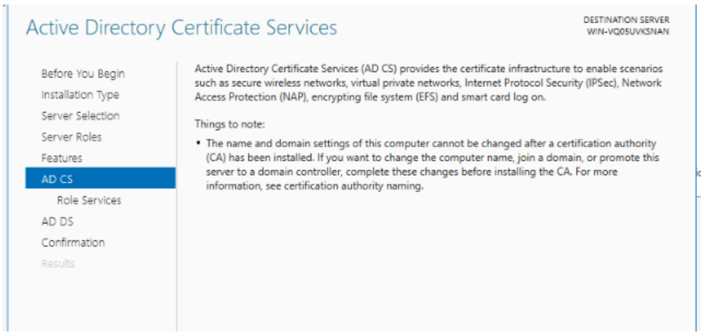
Name	IP Address	Operating System
WIN-S633NS23MP2	10.10.0.1,192.1...	Microsoft Windows Server 2016 Datacenter Evaluation



Roles

▷ ■ Active Directory Certificate Services (2 of 6 installe
☑ Active Directory Domain Services (Installed)
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Device Health Attestation
□ DHCP Server
☑ DNS Server (Installed)
□ Fax Server
▷ ■ File and Storage Services (2 of 12 installed)
□ Host Guardian Service
□ Hyper-V
□ MultiPoint Services
□ Network Controller
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services

Desc
Activ
(AD
certi
role
and
varie



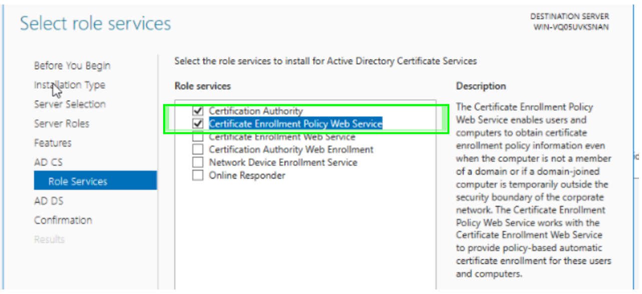
Active Directory Certificate Services

DESTINATION SERVER
WIN-VQ05UVKSNAN

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.



Select role services

DESTINATION SERVER
WIN-VQ05UVKSNAN

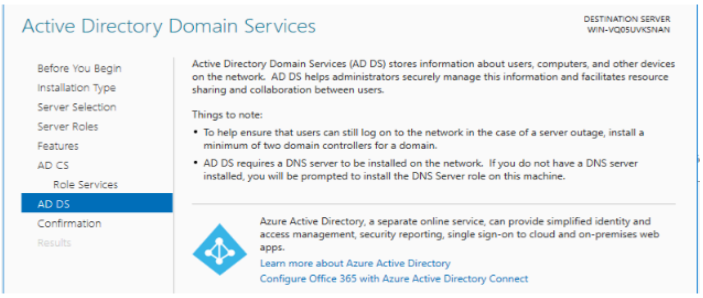
Select the role services to install for Active Directory Certificate Services

Role services

☑ Certification Authority
☑ Certificate Enrollment Policy Web Service
□ Certificate Enrollment Web Service
□ Certification Authority Web Enrollment
□ Network Device Enrollment Service
□ Online Responder

Description

The Certificate Enrollment Policy Web Service enables users and computers to obtain certificate enrollment policy information even when the computer is not a member of a domain or if a domain-joined computer is temporarily outside the security boundary of the corporate network. The Certificate Enrollment Policy Web Service works with the Certificate Enrollment Web Service to provide policy-based automatic certificate enrollment for these users and computers.



Active Directory Domain Services

DESTINATION SERVER
WIN-VQ05UVKSNAN

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

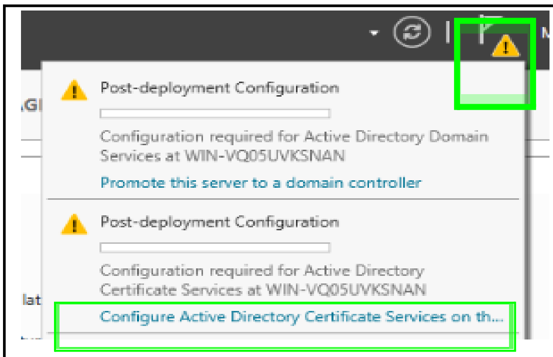
Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect

2. Post-Deployment Configuration

- Access the post-deployment configuration in Server Manager.
- Configure AD CS roles:
  - Select "Certification Authority" and "Certificate Enrollment Policy Web Service".
- Complete the AD DS configuration.
- Configure the Certification Authority:
  - Select "Enterprise CA" , then Choose "Root CA".
  - Create a new private key and Configure encryption options.
  - Define the CA validity period (e.g., 20 years).
  - Configure the database paths.



Post-deployment Configuration

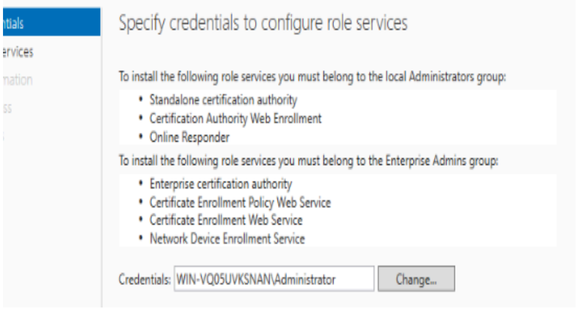
Configuration required for Active Directory Domain Services at WIN-VQ05UVKSNAN

Promote this server to a domain controller

Post-deployment Configuration

Configuration required for Active Directory Certificate Services at WIN-VQ05UVKSNAN

Configure Active Directory Certificate Services on th...



Specify credentials to configure role services

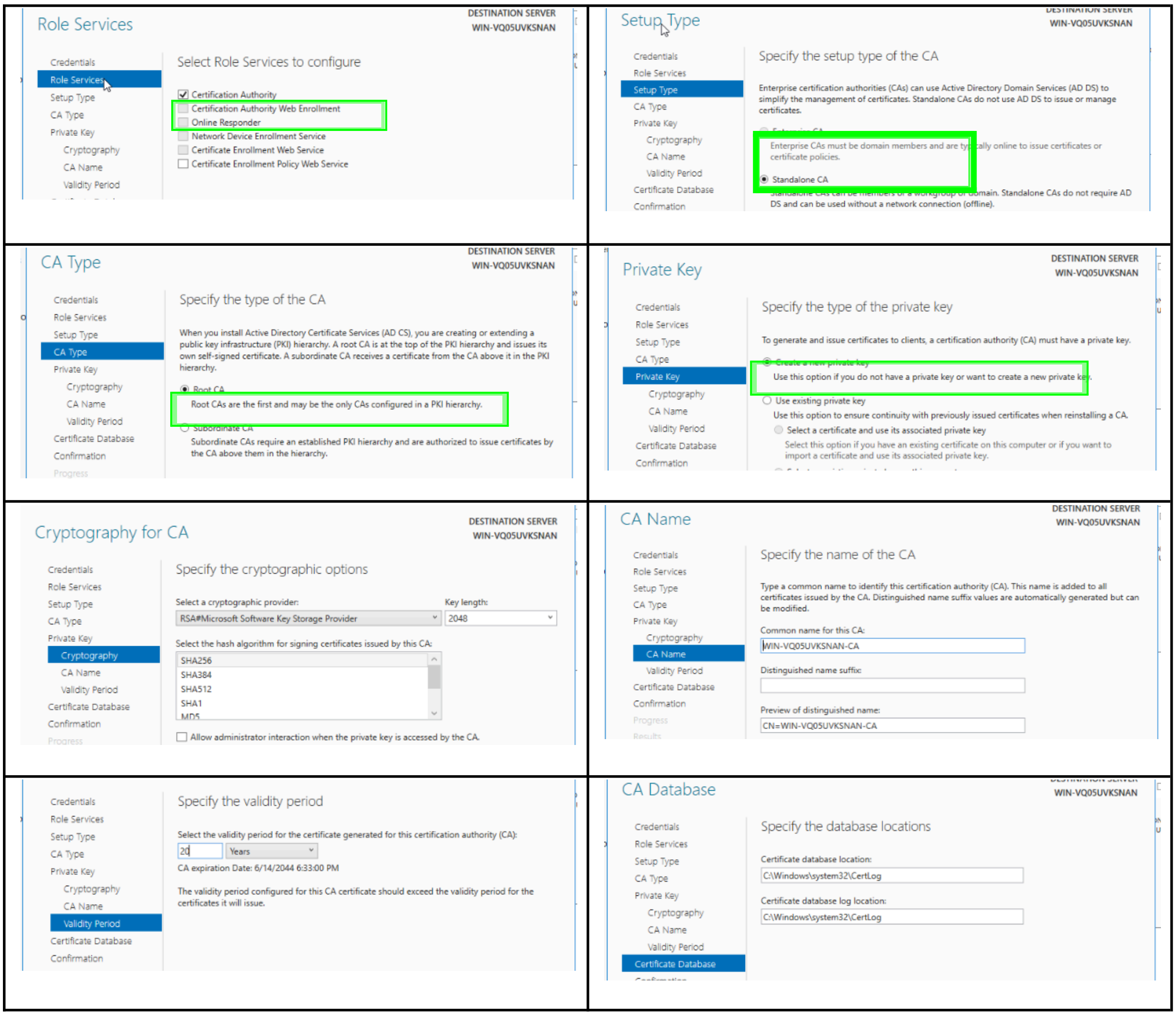
To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: WIN-VQ05UVKSNAN\Administrator



Role Services

DESTINATION SERVER
WIN-VQ05UVKSNAN

Select Role Services to configure

- ☑ Certification Authority
- □ Certification Authority Web Enrollment
- □ Online Responder
- □ Network Device Enrollment Service
- □ Certificate Enrollment Web Service
- □ Certificate Enrollment Policy Web Service

Setup Type

DESTINATION SERVER
WIN-VQ05UVKSNAN

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

○ Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

● Standalone CA

Standalone CAs can be members of a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

CA Type

DESTINATION SERVER
WIN-VQ05UVKSNAN

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.

Private Key

DESTINATION SERVER
WIN-VQ05UVKSNAN

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key

Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key

Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

Cryptography for CA

DESTINATION SERVER
WIN-VQ05UVKSNAN

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

CA Name

DESTINATION SERVER
WIN-VQ05UVKSNAN

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: WIN-VQ05UVKSNAN-CA

Distinguished name suffix:

Preview of distinguished name: CN=WIN-VQ05UVKSNAN-CA

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA): 20 Years

CA expiration Date: 6/14/2044 6:33:00 PM

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

CA Database

WIN-VQ05UVKSNAN

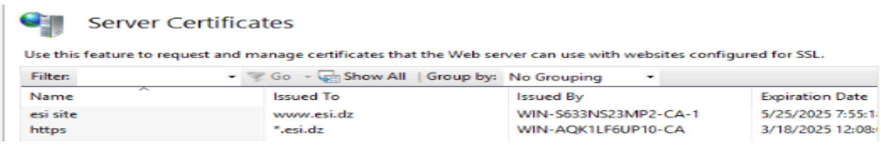
Specify the database locations

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

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

7. Server Certificate Creation and SSL Configuration

On the web server, create a certificate request.



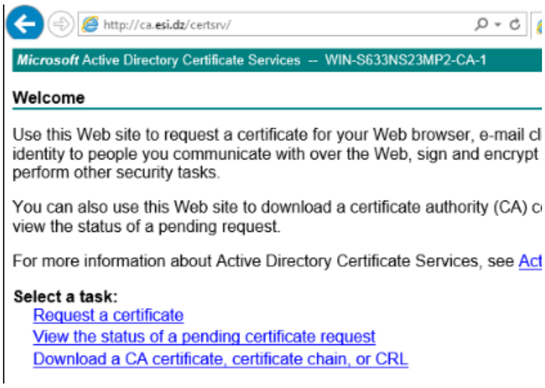
Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	Expiration Date
esi site	www.esi.dz	WIN-S633NS23MP2-CA-1	5/25/2025 7:55:1
https	*.esi.dz	WIN-AQK1LF6UP10-CA	3/18/2025 12:08:

1. Sending the Request to theCA

- Open the site `http://ca.esi.dz/certsrv`.
- Click on "**Request a certificate**" then "**Advanced certificate request**".
- Copy the content of the request file and submit it.



http://ca.esi.dz/certsrv/

Microsoft Active Directory Certificate Services -- WIN-S633NS23MP2-CA-1

Welcome

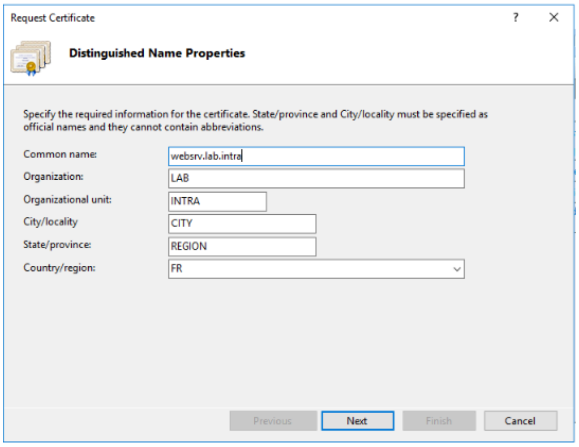
Use this Web site to request a certificate for your Web browser, e-mail cl identity to people you communicate with over the Web, sign and encrypt perform other security tasks.

You can also use this Web site to download a certificate authority (CA) c view the status of a pending request.

For more information about Active Directory Certificate Services, see Act

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL



Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

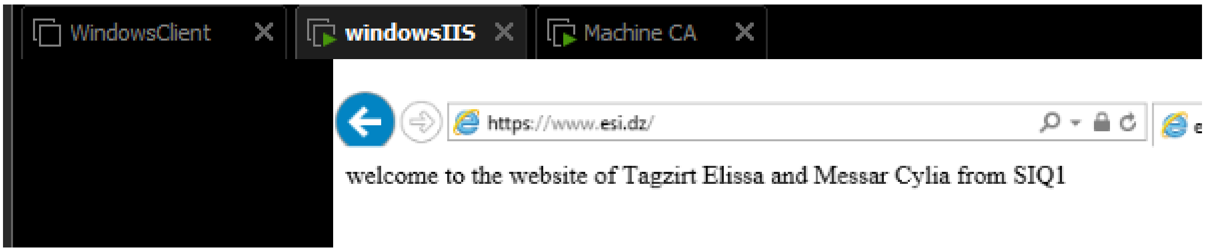
Common name:	websrv.lab.intra
Organization:	LAB
Organizational unit:	INTRA
City/locality:	CITY
State/province:	REGION
Country/region:	FR

2. Certificate Reception and Installation

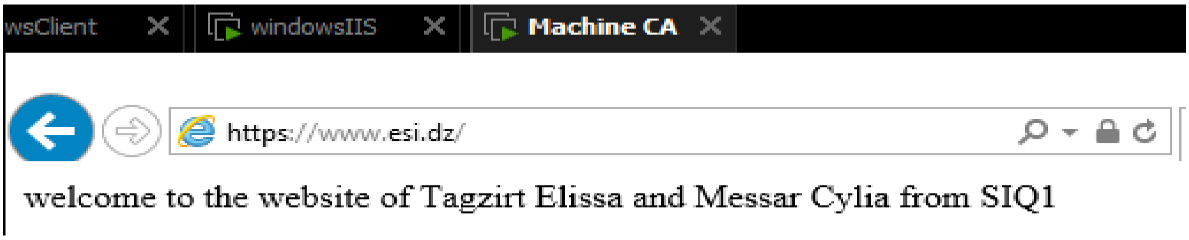
- Receive the certificate issued by the CA.
- Complete the certificate request in IIS.
- Enable HTTPS on the IIS web server.

8. HTTPS Tests

- Use a web browser to access the site via HTTPS: `https://www.esi.dz`.



welcome to the website of Tagzirt Elissa and Messar Cylia from SIQ1



welcome to the website of Tagzirt Elissa and Messar Cylia from SIQ1

Conclusion

Public Key Infrastructure (PKI) is essential for modern cybersecurity, providing strong mechanisms for managing cryptographic keys and digital certificates. It ensures authentication, data integrity, confidentiality, and non-repudiation. By leveraging trusted Certification Authorities (CAs) and Registration Authorities (RAs), PKI secures digital communications through encryption and digital signatures. This robust framework protects against cyber threats, ensuring secure, tamper-proof data exchanges and reliable identity verification. Implementing PKI is crucial for maintaining a secure and trustworthy digital environment.