**Windows Server Configuration Walkthrough**

**1. Environment Setup**

**1.1 Virtual Network Configuration**

* Open VirtualBox and create two network adapters for both the Server and Client VMs:

Adapter 1 (NAT): For internet access.

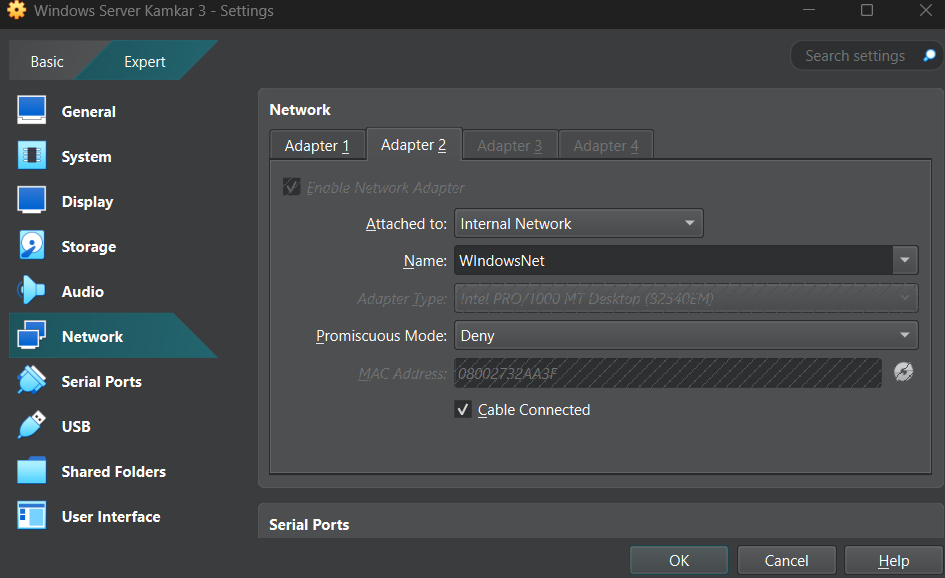
Adapter 2 (Internal Network): For communication between the server and client.

Set the Internal Network name (e.g., WindowsNet).

* For both VMs:

Go to Settings > Network > Adapter 1, and select NAT.

Go to Settings > Network > Adapter 2, and select Internal Network and set the same network name as in step 1.



**2. Install Windows Server 2022 and Client**

Create VMs for:

Server VM: Use at least 4 GB RAM, 1 CPU, and 50 GB storage.

Client VM: Use at least 4 GB RAM, 1 CPU, and 50 GB storage (Windows 10).

Attach respective ISOs to each VM and install Windows Server 2022 and the client OS.

Enable Static IP on the Internal Network adapter for the server:

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: Leave empty.

Configure the client for automatic IP assignment (DHCP).

**3. Configure the Windows Server Roles**

**3.1 Promote to Domain Controller**

Open Server Manager, and add the Active Directory Domain Services (AD DS) role.

After installation, click Promote this server to a domain controller.

Choose Add a new forest, and set:

Root domain: kamkar3.com.

Restart the server after promotion.

**3.2 Create Organizational Units (OUs)**

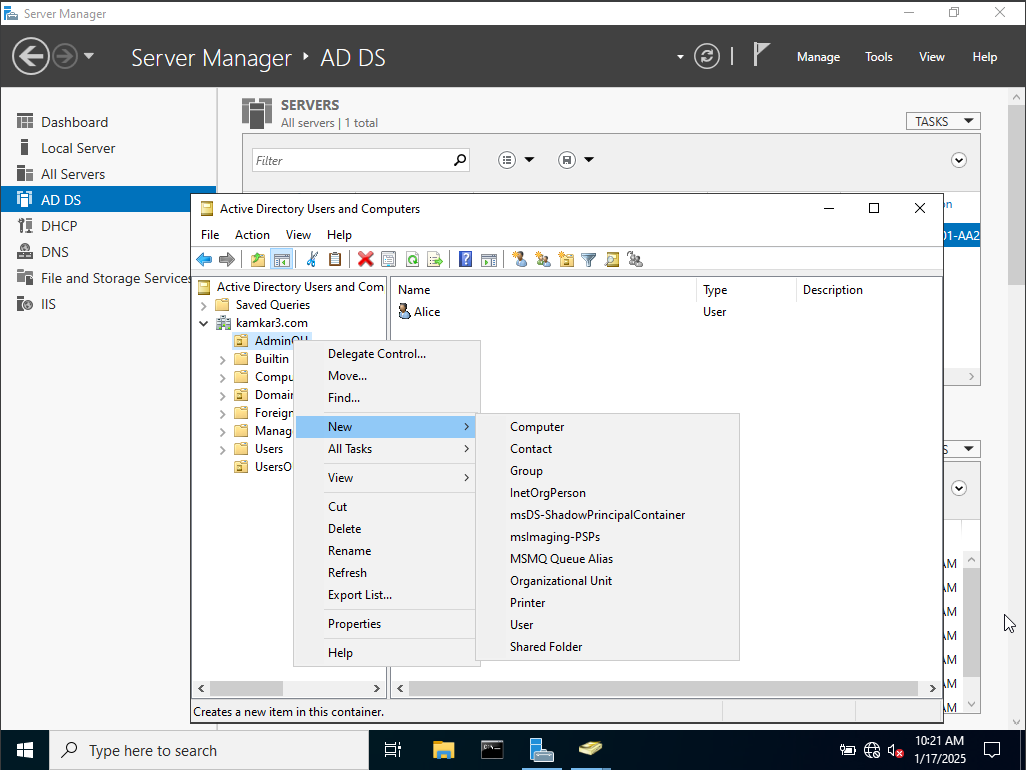
Open Active Directory Users and Computers (ADUC).

Create OUs:

AdminOU: For administrators like Alice.

UsersOU: For standard users like Bob.

Right-click Domain Name > New > Organizational Unit.



**3.3 Add Users (Alice and Bob)**

Create Alice:

Navigate to AdminOU > New > User.

Assign the Domain Admins group to Alice.

Create Bob:

Navigate to UsersOU > New > User.

Assign a home folder path: C:\WIN-7K958PMAP1I\Users\Bob

* **Change Alice's Password**

Log in to the Domain Controller:

Use your administrator account on the Domain Controller.

Open Active Directory Users and Computers:

Press Windows + R, type dsa.msc, and press Enter.

Locate Alice’s Account:

Navigate to the organizational unit (OU) or container where Alice’s account is located.

Example: If Alice is in the Admin OU, look under kamkar3.com > Admin.

Reset the Password:

Right-click Alice’s account and select Reset Password.

Enter a new password that meets the domain's password policy requirements.

Uncheck the "User Must Change Password at Next Logon" Option:

During the reset process, you’ll see a checkbox labeled "User must change password at next logon".

Uncheck this box to allow Alice to log in without being forced to change her password immediately.

Apply and Confirm:

Click OK to save the changes.

**Next -** Join the Client to the Domain:

On the Client Machine:

Log in to the local account.

Open Settings > System > About, and scroll to Domain or Workgroup.

Click Join a Domain.

Enter Domain Information:

In the domain field, enter kamkar3.com.

When prompted, provide Alice's credentials:

Username: KAMKAR3\Alice

Password: Kamkar3

Restart the Machine:

Once the client joins the domain successfully, it will prompt for a restart.

Restart the client machine.

Step 3: Log in as Alice

After Restart:

At the login screen, select Other User.

Log in with Alice’s domain credentials:

Username: KAMKAR3\Alice

Password: Kamkar3

Test Connectivity:

Once logged in, ensure the domain resources (e.g., shared folders, printers) are accessible.

**3.4 Open Group Policy Management**

On your Windows Server:

Open Server Manager.

Navigate to Tools > Group Policy Management.

**Create a GPO for Alice**

In the Group Policy Management console:

Expand your domain name (myadserver.com).

Right-click AdminOU (where Alice's account is located) and select Create a GPO in this domain, and Link it here....

Name the GPO (e.g., Admin Policy for Alice).

Configure the GPO:

Right-click the newly created GPO and select Edit.

The Group Policy Management Editor will open.

Apply specific policies for administrators:

For example, allow Alice to access advanced administrative tools:

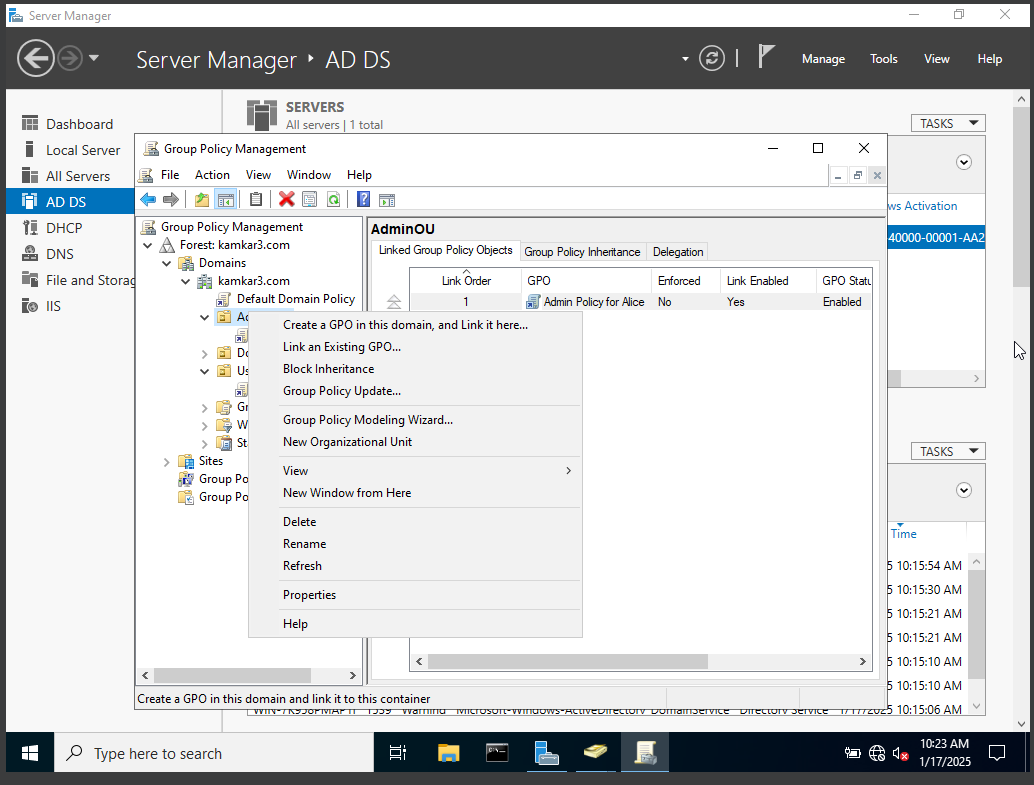
Navigate to User Configuration > Administrative Templates > Control Panel.

Enable Prohibit access to Control Panel and PC settings > Set to Disabled (so she has full access).

Restrict changes to system settings for other users:

Navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment.

Ensure only Domain Admins (including Alice) have rights for sensitive tasks, like Log on locally or Manage auditing and security log.



**Create a GPO for Bob**

Repeat the steps above, but create the GPO under UsersOU.

Name the GPO (e.g., Standard User Policy for Bob).

Configure restrictions for Bob:

Open the GPO in the Group Policy Management Editor.

Apply user restrictions:

Navigate to User Configuration > Administrative Templates > System:

Enable Prevent access to the command prompt.

Enable Run only specified Windows applications and add applications Bob is allowed to use (e.g., notepad.exe, calc.exe, etc.).

Navigate to User Configuration > Start Menu and Taskbar:

Enable Remove access to the Shut Down, Restart, Sleep, and Hibernate commands.

**Apply the GPOs**

Ensure the GPOs are linked to the respective OUs:

Alice's GPO should be linked to AdminOU.

Bob's GPO should be linked to UsersOU.

Test the GPOs:

Log in as Alice and Bob on the client machine to verify the policies are applied.

Use gpresult /r in the command prompt to review applied policies.

**3.5: Install and Configure DNS**

* **Verify DNS Installation**

During Active Directory Domain Services (AD DS) Installation:

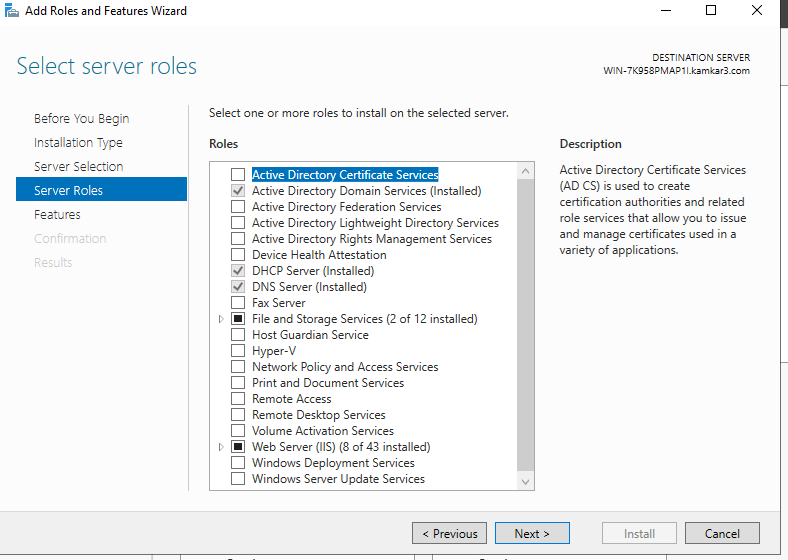
DNS is installed automatically when you promote your server to a Domain Controller.

Verify this by opening Server Manager and checking for the DNS role under the Roles and Features section.

If not installed:

Go to Server Manager > Add Roles and Features.

Select DNS Server under the Server Roles section and complete the installation.



* **Open DNS Manager**

Open DNS Manager:

Go to Server Manager > Tools > DNS.

Expand your server name to view the DNS zones:

Forward Lookup Zones: Resolves domain names to IP addresses.

Reverse Lookup Zones: Resolves IP addresses to domain names (optional but recommended).

* **Configure Forward Lookup Zones**

Create a Primary Zone (if not already created during domain setup):

Right-click Forward Lookup Zones > New Zone.

Choose Primary Zone and ensure it is stored in Active Directory.

Set the zone name as your domain (kamkar3.com).

Allow only secure dynamic updates (recommended for Active Directory).

Verify Existing Records:

Check if the DNS zone already contains the following:

Host (A) Records: Map domain names to IP addresses.

NS Records: Indicate the name servers for the zone.

You should see entries for the domain controller (WIN-7K958PMAP1I).

Step 4: Configure Reverse Lookup Zones (Optional but Recommended)

Add a Reverse Lookup Zone:

Right-click Reverse Lookup Zones > New Zone.

Choose Primary Zone, and ensure it is stored in Active Directory.

Specify the network ID (e.g., 192.168.1 for your internal network).

Allow only secure dynamic updates.

* **Verify:**

Ensure the reverse zone resolves IP addresses to domain names:

Add a PTR (Pointer) record mapping your domain controller's IP to its name.

* **Test DNS Configuration**

Open a command prompt and test DNS queries using nslookup:

Query your domain:

nslookup kamkar3.com

Query your domain controller:

nslookup WIN-7K958PMAP1I.kamkar3.com

If conditional forwarders are configured, test external queries:

*nslookup google.com*

* **Integrate DNS with Active Directory**

Active Directory automatically integrates with DNS to ensure proper domain functionality. If the DNS server is running on your domain controller, this step is completed during promotion.

=======================================================

**Step 3.6: Install and Configure DHCP**

The Dynamic Host Configuration Protocol (DHCP) allows your server to assign IP addresses automatically to devices on your network. Below are the steps to install and configure DHCP on Windows Server 2022.

* **Install DHCP Server Role**

Open Server Manager.

Click Manage > Add Roles and Features.

Add Roles and Features Wizard:

Click Next until you reach the Server Roles screen.

Select DHCP Server and click Next.

Complete the wizard and click Install.

Once installed:

Click Complete DHCP Configuration in Server Manager.

* **Authorize the DHCP Server**

During the configuration wizard:

Select Use current credentials or specify a domain administrator account.

Click Commit to authorize the DHCP server in Active Directory.

Verify authorization:

Open the DHCP Management Console:

Go to Tools > DHCP in Server Manager.

Ensure your server name shows with a green checkmark.

* **Configure a DHCP Scope**

Open the DHCP Management Console.

Right-click your server name and select New Scope.

New Scope Wizard:

Scope Name: Enter a name (MyScope).

IP Address Range: Enter the range of IP addresses to be assigned (192.168.1.10 to 192.168.1.20).

Subnet Mask: Typically 255.255.255.0 for a standard Class C network.

Lease Duration: Default is 8 days; adjust if necessary.

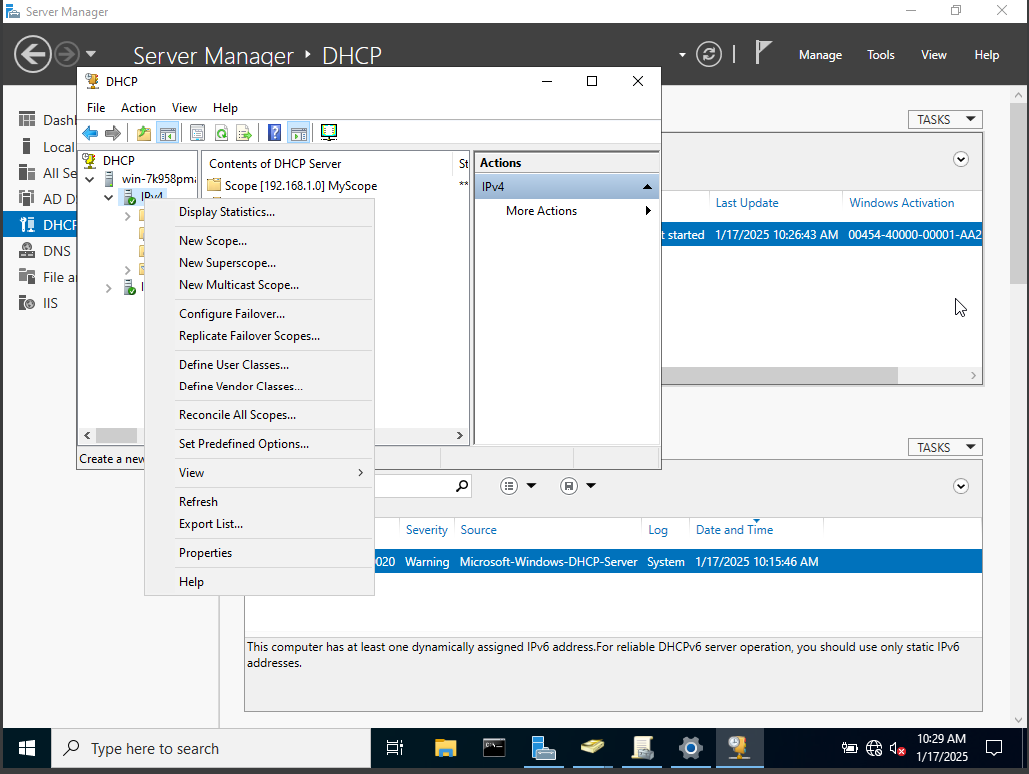
Configure DHCP Options:

Router (Default Gateway): Enter your gateway’s IP (192.168.1.1).

DNS Servers: Enter the server’s IP address (192.168.1.1) and optionally an external DNS (e.g., 8.8.8.8).

Complete the wizard:

Activate the scope when prompted.



* **Test the DHCP Server**

Restart DHCP Service:

Open a command prompt and restart the DHCP service:

net stop dhcpserver && net start dhcpserver

Check Client Configuration:

On a client VM connected to the server's network:

Ensure the network adapter is set to Obtain an IP address automatically.

Run the following command to verify DHCP assignment:

*ipconfig /renew*

Check the assigned IP and ensure it falls within the configured scope.

Verify Leases:

In the DHCP Management Console, expand your scope and check Address Leases for assigned IPs.

* **Integrate DHCP with Active Directory (Optional)**

Configure dynamic DNS updates for DHCP-assigned clients:

In the DHCP Management Console, right-click your scope and select Properties.

Go to the DNS tab and select:

Enable DNS dynamic updates according to the settings below.

Check Always dynamically update DNS A and PTR records.

Click OK.

* **Test and Verify**

On the client VM, verify:

The client receives an IP address automatically.

The default gateway and DNS settings are correct.

Test connectivity:

Ping the server by its IP address and domain name to verify DNS integration.

**Step 3.7: Install and Configure IIS (Internet Information Services) for Alice**

Internet Information Services (IIS) is a web server role that allows you to host web applications and services on Windows Server. Below are the steps to install and configure IIS on Windows Server 2022.

* **Install the IIS Role**

Open Server Manager.

Click Manage > Add Roles and Features.

Add Roles and Features Wizard:

Click Next until you reach the Select Features screen.

On the Select Roles screen, check Web Server (IIS).

Click Next until you reach the Select Features screen, and leave the default features unless you need additional ones.

Complete the wizard and click Install.

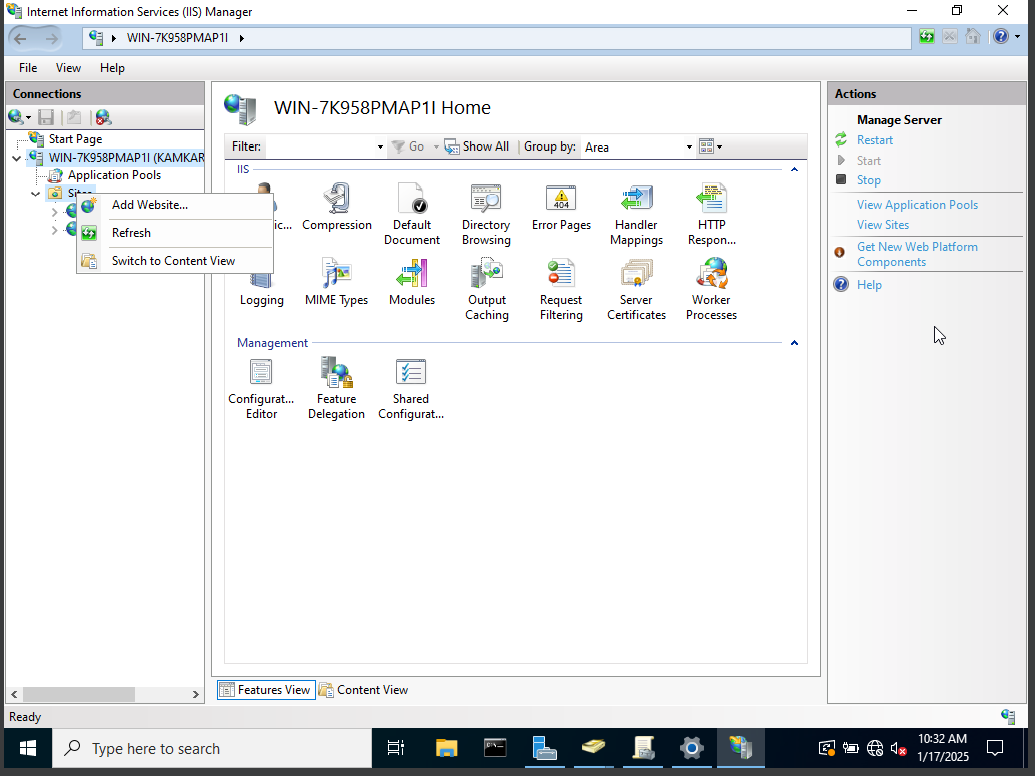
Verify IIS Installation:

Once installed, go to Server Manager > Tools > Internet Information Services (IIS) Manager.

* **Configure IIS for Alice's Web Application**

Open IIS Manager:

Click Start > Administrative Tools > Internet Information Services (IIS) Manager.



Create a New Website:

In the IIS Manager, under your server name, right-click Sites and select Add Website.

Site Name: Enter a name for the site (e.g., Kamkar3).

Physical Path: Set the path to the folder containing Alice’s web application (e.g., C:\inetpub\wwwroot\Kamkar3).

Binding: Set the port (usually 80 for HTTP) and the hostname (e.g., alice.myadserver.com).

Click OK.

Set Permissions:

Ensure that the directory where Alice’s application is stored has appropriate permissions for IIS to access it. Right-click the folder > Properties > Security tab and ensure that IIS\_IUSRS has read permissions.

Verify Website Access:

From a browser on a client VM or the server, enter the website URL (e.g., http://alice.myadserver.com).

Ensure the web application loads correctly.

* **Secure IIS**

Enable Windows Authentication :

In IIS Manager, go to Sites > Kamkar3 > Authentication.

Enable Windows Authentication if your app uses domain credentials.

Configure SSL:

In IIS, under Sites > Kamkar3, select Bindings > Add.

Choose https and select a valid SSL certificate for your domain.

Apply Additional Security:

Use Request Filtering in IIS to block unwanted requests.

Consider enabling a Web Application Firewall (WAF) for added protection.

* **Test the Web Application**

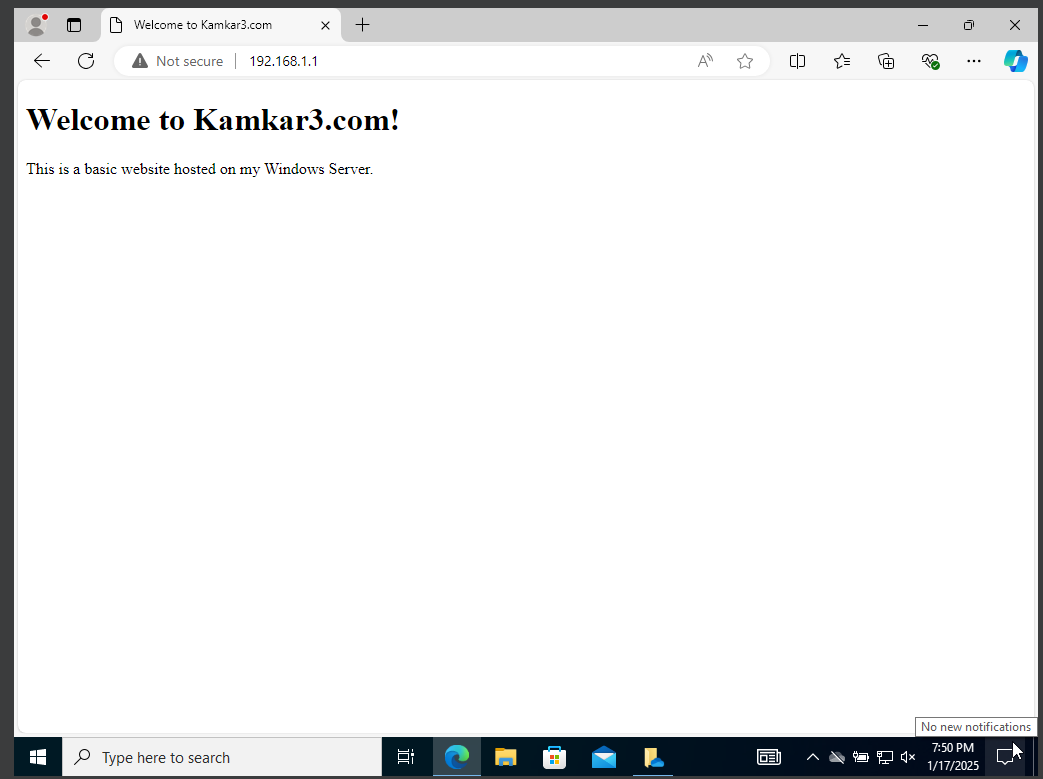
Test Access:

On a client VM in your domain, open a browser and type http://alice.kamkar3.com (or use localhost or the server's IP if necessary).

Confirm that Alice's web application is accessible.

Test Authentication:

Ensure that Alice can log in to the web app with her domain credentials, based on IIS’s security settings.



* **Configure DNS for IIS (Optional)**

Set up DNS for the Website:

If you want to access Alice’s web application using a domain name, add an A record in the DNS server.

Open DNS Manager.

Under Forward Lookup Zones, right-click the domain (kamkar3.com) > New Host (A or AAAA).

Name: alice (this will make it alice.kamkar3.com).

IP Address: The server’s IP address.

Test DNS Resolution:

From a client machine, run:

*nslookup alice.kamkar3.com*

Ensure it resolves to the correct IP address.

* **Change the Default Website Binding**

This option is useful if you want to use the current default website (e.g., Default Web Site) but change its settings to serve your new content.

Open IIS Manager:

Press Windows + R, type inetmgr, and press Enter to open IIS Manager.

Select the Default Website:

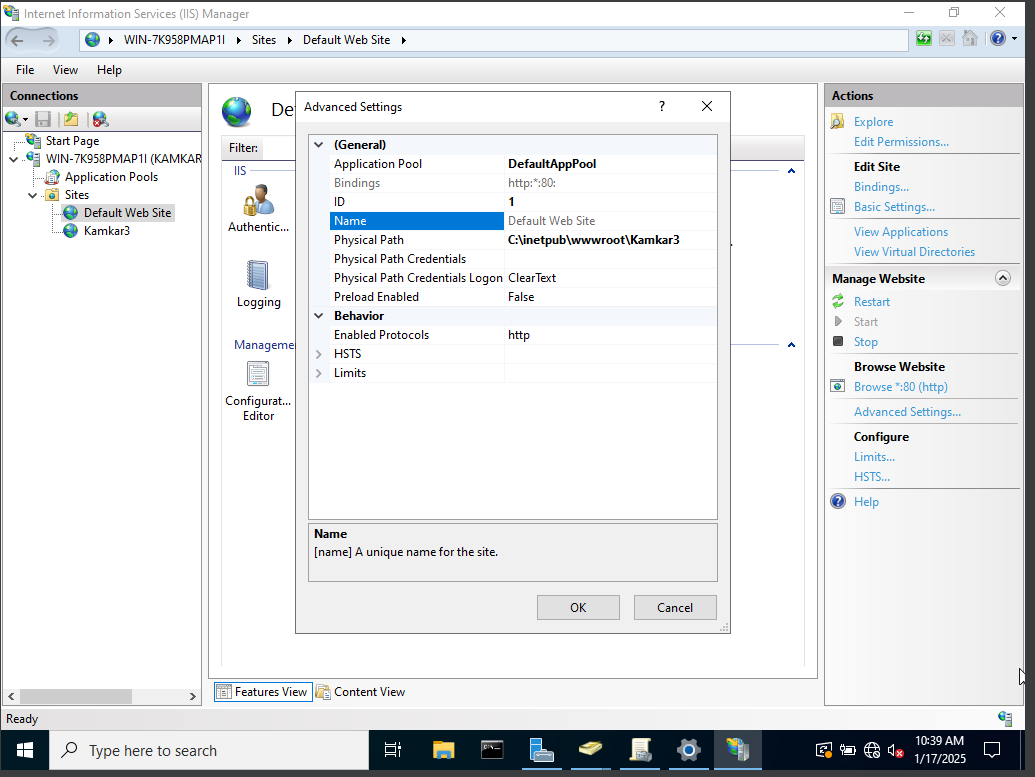
In the Connections pane (left side), expand the server node and click on Sites.

You’ll see the list of websites hosted on your server. The Default Web Site is typically the first one listed.

Change the Default Website’s Physical Path:

Right-click Default Web Site, and choose Manage Website > Advanced Settings.

Under the Physical Path section, click on the ... button to browse and select the new folder where your website files are located (e.g., C:\inetpub\wwwroot\kamkar3.com).



Change the Website Bindings:

Right-click Default Web Site, and select Edit Bindings.

In the Site Bindings window, you can change the port, IP address, or hostname used by the website. For example, if you want kamkar3.com to be the default, set it in the Host Name field.

Port: Ensure it’s set to 80 (or 443 for HTTPS).

Host Name: If needed, add your domain (e.g., kamkar3.com).

Restart IIS:

After making changes, you might need to restart IIS to apply them. Right-click Default Web Site and select Restart.