**UNITY UNIVERSITY, ADAMA CAMPUS**

**DEPARTMENT OF COMPUTER SCIENCE**

**LAB PROJECT FOR SYSTEM AND NETWOR ADMINISTRATION (COSC4081)**

1. **To Install Windows Server 2021**

**Part 1: Preparing the Environment**

1. **Verify Requirements:**
   * Ensure the hardware or VM meets the minimum requirements.
   * If using a physical computer, insert the bootable media (USB/DVD).
   * For VMs, attach the ISO file to the virtual drive.
2. **Configure BIOS/UEFI Settings:**
   * Restart the system and access the BIOS/UEFI settings (usually by pressing a key like F2, F10, DEL, or ESC during boot).
   * Set the boot order to prioritize the USB/DVD drive or virtual drive containing the Windows Server 2021 installation media.
   * Save changes and exit BIOS/UEFI.

2.  **Installing Windows Server 2021**

**3. Post-Installation Configuration**

1. **Set Administrator Password:**
   * After installation, you’ll be prompted to set a password for the Administrator account. Use a strong password.
2. **Log In:**
   * Use the Administrator account to log in.
3. **Configure Initial Settings:**
4. Activate Windows Server:
5. Install Updates
6. Join a Domain (Optional)
7. **Assign a Domain Name to Windows Server**

**Prerequisites:**

* A clean installation of Windows Server.
* Administrator privileges on the server.
* A static IP address assigned to the server.

**Step 1: Set a Static IP Address**

 Open **Control Panel > Network and Sharing Center**.

 Click **Change adapter settings** on the left-hand panel.

 Right-click your active network adapter and select **Properties**.

 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

 Choose **Use the following IP address**:

* **IP Address:** Assign a unique IP address for your server (e.g., 192.168.1.10).
* **Subnet Mask:** Typically 255.255.255.0.
* **Default Gateway:** Your network's gateway (e.g., 192.168.1.1).
* **Preferred DNS Server:** Use the server’s IP address (e.g., 192.168.1.10).

 Click **OK** and close the dialog boxes.

**Step 2: Install the Active Directory Domain Services (AD DS) Role**

1. Open **Server Manager** from the Start menu.
2. Click **Add roles and features** in the Dashboard.
3. In the **Add Roles and Features Wizard**:
   * Select **Role-based or feature-based installation** and click **Next**.
   * Choose the local server and click **Next**.
   * Select **Active Directory Domain Services**, and click **Add Features** when prompted.
   * Click **Next** and then **Install**.
4. Wait for the installation to complete, but **do not restart** yet.

**Step 3: Promote the Server to a Domain Controller**

1. In **Server Manager**, click the **Notification Flag** in the upper-right corner and select **Promote this server to a domain controller**.
2. In the **Active Directory Domain Services Configuration Wizard**:
   * **Deployment Configuration:** Choose one of the following:
     + **Add a new forest** if you're creating a new domain (e.g., example.local).
     + **Add a domain to an existing forest** if joining an existing structure.
   * Enter the fully qualified domain name (FQDN) for your domain (e.g., example.local) and click **Next**.
3. **Domain Controller Options:**
   * Choose a **Forest Functional Level** and **Domain Functional Level** (e.g., Windows Server 2021).
   * Check **DNS Server** and **Global Catalog (GC)**. Leave the **Read-only domain controller (RODC)** unchecked.
   * Set a **Directory Services Restore Mode (DSRM) password**.
   * Click **Next**.
4. **DNS Options:** Click **Next** (ignore any delegation warnings for now).
5. **Additional Options:**
   * Confirm the NetBIOS domain name (e.g., EXAMPLE) and click **Next**.
6. **Paths:** Leave the default paths for the database, log files, and SYSVOL shared folder. Click **Next**.
7. **Review Options:** Review your selections and click **Next**.
8. **Prerequisites Check:** Allow the wizard to check prerequisites. If there are no critical errors, click **Install**.

**Step 4: Restart the Server**

* After the promotion process is complete, the server will restart automatically.

**Step 5: Verify the Domain Configuration**

1. Log in using the domain Administrator account.
   * Username: DOMAIN\Administrator (e.g., EXAMPLE\Administrator).
   * Password: Use the password set during installation.
2. Open **Server Manager** and verify:
   * The domain name is listed in **Active Directory Users and Computers**.
   * The DNS server is functioning correctly under **DNS Manager**.

**Step 6: Add Computers to the Domain (Optional)**

1. On a client machine, go to **System > About > Rename this PC (advanced)**.
2. Click **Change** under **Computer Name**.
3. Select **Domain**, enter the domain name (e.g., example.local), and click **OK**.
4. Enter domain Administrator credentials when prompted.
5. Restart the client machine to apply the changes.

**Steps to Install and Configure DHCP on Windows Server**

**Step 1: Prerequisites**

1. Ensure the server has a static IP address configured.
2. Verify that the server is a member of a domain (if required for your setup).
3. Administrator privileges are required to perform these steps.

**Step 2: Install the DHCP Server Role**

1. **Open Server Manager:**
   * Press Windows + R, type ServerManager, and press Enter.
2. **Add the DHCP Role:**
   * In Server Manager, click **Add roles and features**.
   * Choose **Role-based or feature-based installation** and click **Next**.
   * Select the server from the server pool and click **Next**.
   * Check **DHCP Server** and click **Add Features** when prompted.
   * Click **Next** through the wizard and then **Install**.
3. **Complete Installation:**
   * Wait for the installation to complete. Do not restart the server yet.
4. **Post-Deployment Configuration:**
   * In Server Manager, click the **Notification Flag** in the upper-right corner.
   * Select **Complete DHCP Configuration**.

**Step 3: Configure DHCP Post-Installation**

1. **Authorization:**
   * In the **DHCP Post-Install Wizard**, choose to authorize the DHCP server in Active Directory (for domain environments).
   * Use domain Administrator credentials if prompted.
2. **Close the Wizard:**
   * Once completed, close the wizard.

**Step 4: Configure DHCP Scopes**

A DHCP scope defines the range of IP addresses the server can lease to clients.

1. **Open DHCP Management Console:**
   * Press Windows + R, type dhcpmgmt.msc, and press Enter.
2. **Create a New Scope:**
   * In the left-hand pane, right-click the **IPv4** node and select **New Scope**.
   * Follow the New Scope Wizard:
     + **Name and Description:** Enter a name (e.g., "Office LAN Scope") and optional description.
     + **IP Range:** Specify the range of IP addresses for the scope (e.g., 192.168.1.100 to 192.168.1.200).
     + **Subnet Mask:** Set the subnet mask (e.g., 255.255.255.0).
     + **Exclusions (Optional):** Specify any IPs within the range that should not be leased (e.g., reserved for static addresses).
     + **Lease Duration:** Set how long a client can use an IP address before it must be renewed (default is 8 days).
     + **DHCP Options:** Configure options such as:
       - **Router (Default Gateway):** Enter the IP address of the gateway (e.g., 192.168.1.1).
       - **Domain Name and DNS Servers:** Enter your domain name (e.g., example.local) and DNS server IP address (e.g., 192.168.1.10).
     + **Activate Scope:** Select **Yes, I want to activate this scope now**.
3. **Complete Scope Configuration:**
   * Click **Finish** to save the scope.

**Step 5: Start the DHCP Server**

1. In the **DHCP Management Console**, ensure the server is running.
2. If it is stopped, right-click the server node and select **Start**.

**Step 6: Verify DHCP Operation**

1. **Test IP Address Allocation:**
   * Connect a client device to the network and ensure it obtains an IP address dynamically.
   * On the client device, run ipconfig /renew in Command Prompt to request a new IP address.
   * Run ipconfig to verify the assigned IP and settings.
2. **Monitor Leases:**
   * In the DHCP Management Console, expand the IPv4 node and click **Address Leases** to view the devices that have obtained IP addresses.

**Troubleshooting Tips**

* **Scope Exhausted:** Ensure the scope has sufficient IPs for all devices.
* **Authorization Issues:** Reauthorize the DHCP server in Active Directory using the DHCP Management Console.
* **Clients Not Receiving IPs:** Verify that the DHCP server is running and connected to the same network as the clients.

**Steps to Install and Configure an FTP Server on Windows Server**

**Step 1: Prerequisites**

1. A Windows Server system with administrative privileges.
2. A static IP address assigned to the server (optional but recommended).
3. Ensure IIS (Internet Information Services) is not already configured if installing FTP on a fresh server.

**Step 2: Install the FTP Server Role**

1. **Open Server Manager:**
   * Press Windows + R, type ServerManager, and press Enter.
2. **Add the Web Server (IIS) Role:**
   * Click **Add Roles and Features** in the Server Manager Dashboard.
   * Choose **Role-based or feature-based installation** and click **Next**.
   * Select the local server from the server pool and click **Next**.
   * Expand **Web Server (IIS)** and select **FTP Server**.
     + Check **FTP Service** and **FTP Extensibility**.
   * Click **Next**, then **Install**.
3. **Wait for Installation:**
   * Allow the process to complete. Once installed, click **Close**.

**Step 3: Configure the FTP Server**

1. **Open IIS Manager:**
   * Press Windows + R, type inetmgr, and press Enter.
2. **Add an FTP Site:**
   * In the IIS Manager, expand the server node in the left-hand pane.
   * Right-click **Sites** and select **Add FTP Site**.
   * Enter the following:
     + **FTP Site Name:** Provide a descriptive name (e.g., "MyFTPSite").
     + **Content Directory:** Specify the physical path where FTP files will be stored (e.g., C:\FTPFolder).
3. **Configure Binding and SSL:**
   * **IP Address:** Choose the server's IP address or leave it as "All Unassigned."
   * **Port:** Enter the FTP port (default is 21).
   * **SSL:** Choose one of the following options:
     + **No SSL:** If secure connections are not required.
     + **Require SSL:** If you have an SSL certificate configured (recommended for secure connections).
4. **Set Authentication and Authorization:**
   * **Authentication:**
     + Enable **Basic Authentication**.
   * **Authorization:**
     + Choose **Specified users**, **All users**, or **Anonymous** depending on your requirements.
     + Set permissions for **Read** and/or **Write** access.
5. **Complete the Wizard:**
   * Click **Finish** to create the FTP site.

**Step 4: Configure Windows Firewall**

1. Open **Control Panel > System and Security > Windows Defender Firewall**.
2. Click **Advanced Settings**.
3. In the **Inbound Rules** section:
   * Add a new rule for FTP:
     + Select **Port** and click **Next**.
     + Enter **21** (or your custom FTP port) and click **Next**.
     + Allow the connection and click **Next**.
     + Name the rule (e.g., "FTP Server Port 21") and click **Finish**.
   * Add another rule for **FTP Data Channel** (Port 20 if passive mode is not configured).

**Step 5: Test the FTP Server**

1. Use an FTP client (e.g., FileZilla) or a web browser to connect:
   * Enter the server's IP address (e.g., ftp://192.168.1.10) and port.
   * Log in with the credentials of an authorized user.
2. Upload or download files to test the functionality.

**Step 6: (Optional) Enable Passive Mode**

1. Open IIS Manager, select the FTP site, and click **FTP Firewall Support**.
2. Configure the **Data Channel Port Range** (e.g., 50000-51000).
3. Update the Windows Firewall to allow the passive mode port range.

**Step 7: (Optional) Configure Virtual Directories**

1. In IIS Manager, right-click the FTP site and select **Add Virtual Directory**.
2. Enter an alias (e.g., "SharedFiles") and specify the physical path (e.g., C:\Shared).
3. Set permissions for the directory.

**Troubleshooting**

* **Connection Refused:** Check the firewall rules and ensure FTP services are running.
* **Authentication Failed:** Verify user credentials and ensure the user has permissions for the FTP site.
* **SSL Errors:** Ensure a valid SSL certificate is installed if SSL is required.

**Steps to Install and Configure IIS on Windows Server**

**Step 1: Prerequisites**

1. A Windows Server machine with Administrator privileges.
2. Static IP address for the server (optional but recommended for production environments).
3. Network connectivity if downloading additional IIS features.

**Step 2: Install the IIS Role**

1. **Open Server Manager:**
   * Press Windows + R, type ServerManager, and press Enter.
2. **Add the IIS Role:**
   * Click **Add Roles and Features** in the Dashboard.
   * Choose **Role-based or feature-based installation** and click **Next**.
   * Select the local server from the server pool and click **Next**.
   * In the **Roles** section, select **Web Server (IIS)**.
     + Click **Add Features** when prompted to add IIS Management Console.
3. **Add Additional Features (Optional):**
   * Click **Next** on the **Features** page to add any additional Windows Server features as needed (e.g., .NET Framework or FTP Server).
4. **Select IIS Role Services:**
   * Review and select the desired IIS role services. Key components include:
     + **Common HTTP Features** (e.g., Static Content, Default Document).
     + **Application Development** (e.g., ASP.NET, .NET Extensibility).
     + **Security** (e.g., Basic Authentication, Windows Authentication).
     + **Performance** (e.g., Static Content Compression).
   * Click **Next** when done.
5. **Install IIS:**
   * Review your selections and click **Install**.
   * Wait for the installation to complete. Click **Close** when done.

**Step 3: Verify IIS Installation**

1. **Open a Web Browser:**
   * Type http://localhost or the server's IP address (e.g., http://192.168.1.10) in the address bar.
   * If IIS is installed correctly, you should see the default IIS welcome page.

**Step 4: Configure IIS**

1. **Open IIS Manager:**
   * Press Windows + R, type inetmgr, and press Enter.
2. **Add a New Website:**
   * In the IIS Manager, expand the server node in the left-hand pane.
   * Right-click **Sites** and select **Add Website**.
   * Provide the following information:
     + **Site Name:** Enter a descriptive name (e.g., "MyWebsite").
     + **Physical Path:** Specify the folder where your website files are stored (e.g., C:\inetpub\wwwroot\MyWebsite).
     + **Binding:** Select the IP address, port (default is 80), and hostname (optional).
   * Click **OK** to create the site.
3. **Set Default Document (Optional):**
   * In IIS Manager, select the site.
   * Double-click **Default Document** and add or prioritize your main file (e.g., index.html or default.aspx).

**Step 5: Configure Firewall for IIS**

1. Open **Control Panel > System and Security > Windows Defender Firewall**.
2. Click **Advanced Settings**.
3. In the **Inbound Rules** section:
   * Add a new rule for IIS:
     + Select **Port** and click **Next**.
     + Enter **80** for HTTP or **443** for HTTPS and click **Next**.
     + Allow the connection and click **Next**.
     + Name the rule (e.g., "IIS HTTP Port 80") and click **Finish**.

**Step 6: Enable HTTPS (Optional)**

1. **Install an SSL Certificate:**
   * Obtain an SSL certificate from a trusted Certificate Authority (CA) or generate a self-signed certificate.
   * In IIS Manager, click the server node, double-click **Server Certificates**, and import or create the certificate.
2. **Bind HTTPS to the Site:**
   * Select the site in IIS Manager and click **Bindings** in the right-hand pane.
   * Click **Add**, select **HTTPS**, and choose the SSL certificate.
   * Click **OK** to save the binding.

**Step 7: Test the Website**

1. Open a web browser and access your site using the server's IP address or hostname.
   * For HTTP: http://192.168.1.10 or http://yourdomain.com.
   * For HTTPS: https://192.168.1.10 or https://yourdomain.com (if SSL is configured).
2. Verify the website loads and displays the intended content.

**Troubleshooting Tips**

* **No Welcome Page:** Ensure the IIS service is running by checking **Services** (services.msc) for "World Wide Web Publishing Service."
* **Access Denied Errors:** Check NTFS permissions on the website folder.
* **Firewall Blocked:** Verify that inbound rules for port 80 (HTTP) or 443 (HTTPS) are configured correctly.
* **Binding Conflicts:** Ensure no other services are using the same IP and port as IIS.

**Steps to Install and Configure a Print Server on Windows Server**

**Step 1: Prerequisites**

1. A Windows Server with administrative privileges.
2. Printers connected to the network or server (either physically or via a network interface).
3. Printer drivers for your printers, compatible with Windows Server.

**Step 2: Install the Print Server Role**

1. **Open Server Manager:**
   * Press Windows + R, type ServerManager, and press Enter.
2. **Add the Print and Document Services Role:**
   * In Server Manager, click **Add roles and features**.
   * Select **Role-based or feature-based installation** and click **Next**.
   * Select the server from the server pool and click **Next**.
   * In the **Roles** section, select **Print and Document Services**.
     + Click **Add Features** when prompted.
   * Expand **Print and Document Services** and select **Print Server**.
   * Click **Next**, review your selections, and click **Install**.
3. **Complete the Installation:**
   * Wait for the installation to complete. Click **Close** when done.

**Step 3: Configure the Print Server**

1. **Open Print Management Console:**
   * Press Windows + R, type printmanagement.msc, and press Enter.
2. **Add Printers:**
   * In the left-hand pane, expand **Print Servers**, then click your server name.
   * Right-click **Printers** and select **Add Printer**.
   * In the Add Printer Wizard:
     + **Add a network, wireless, or Bluetooth printer:** If the printer is on the network.
     + **Add a new printer using an existing port:** For locally connected printers.
   * Select the printer or enter its IP address/hostname.
   * Install the necessary printer driver if prompted.
3. **Share the Printer:**
   * During the wizard, select **Share this printer** and provide a share name.
   * Optionally, add location and comment details for easier identification.

**Step 4: Install Printer Drivers for Clients (Optional)**

1. In the **Print Management Console**, right-click **Drivers** under your Print Server.
2. Select **Add Driver** and use the wizard to add drivers for various operating systems (e.g., 32-bit and 64-bit versions).

**Step 5: Configure Printer Properties (Optional)**

1. In the **Print Management Console**, right-click the printer and select **Properties**.
2. Configure settings such as:
   * **Paper size, print quality, and default settings.**
   * **Security permissions** to control who can print, manage, or configure the printer.

**Step 6: Test the Printer**

1. On the server, right-click the printer in the **Print Management Console** and select **Printer Properties**.
2. Go to the **General** tab and click **Print Test Page** to verify the printer is working.

**Step 7: Allow Client Computers to Access the Printer**

1. Ensure the printer is shared and visible on the network.
2. Open **Control Panel > System and Security > Windows Defender Firewall > Advanced Settings**.
3. Add an inbound rule to allow traffic for **File and Printer Sharing**.

**Step 8: Connect Clients to the Printer**

1. On a client machine:
   * Open **Control Panel > Devices and Printers** and click **Add a Printer**.
   * Select **Add a network, wireless, or Bluetooth printer**.
   * Locate the shared printer by name or browse for it on the network.
2. Install the printer driver if prompted and finish the setup.

**Troubleshooting**

* **Printer Not Listed:** Ensure the printer is powered on and correctly connected to the server or network.
* **Driver Issues:** Verify that compatible printer drivers are installed on the server.
* **Access Denied:** Check the printer's sharing and security settings to ensure appropriate permissions.
* **Firewall Blocking:** Ensure the **File and Printer Sharing** firewall rule is enabled.

**Steps to Configure Group Policy Management on a Domain Controller**

**Step 1: Prerequisites**

1. Ensure the server is a domain controller with the Active Directory Domain Services (AD DS) role installed.
2. Verify you have administrative privileges on the server.

**Step 2: Install the Group Policy Management Console (GPMC)**

1. **Open Server Manager:**
   * Press Windows + R, type ServerManager, and press Enter.
2. **Add Features:**
   * Click **Add Roles and Features**.
   * Choose **Role-based or feature-based installation** and click **Next**.
   * Select the server from the server pool and click **Next**.
   * In the **Features** section, check **Group Policy Management**.
   * Click **Next** and then **Install**.
3. **Verify Installation:**
   * Wait for the installation to complete and ensure **Group Policy Management Console** is available.

**Step 3: Open Group Policy Management Console**

1. Press Windows + R, type gpmc.msc, and press Enter.
2. This opens the **Group Policy Management Console**, where you can manage Group Policy Objects (GPOs).

**Step 4: Create a New GPO**

1. In the **Group Policy Management Console**, expand the forest and domain nodes in the left-hand pane.
2. Right-click the **Group Policy Objects** folder and select **New**.
3. Provide a descriptive name for the new GPO (e.g., "Password Policy") and click **OK**.

**Step 5: Link the GPO to an Organizational Unit (OU)**

1. Navigate to the domain or an Organizational Unit (OU) where you want to apply the GPO.
2. Right-click the domain/OU and select **Link an Existing GPO**.
3. Select the GPO you created from the list and click **OK**.

**Step 6: Edit the GPO**

1. In the **Group Policy Management Console**, right-click the GPO you created and select **Edit**.
2. The **Group Policy Management Editor** opens. Here, you can configure settings in two main categories:
   * **Computer Configuration:** Policies that apply to computers (e.g., security settings, software installations).
   * **User Configuration:** Policies that apply to user accounts (e.g., desktop settings, logon scripts).

**Step 7: Common Configuration Examples**

1. **Enforce Password Policy:**
   * Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.
   * Configure settings such as minimum password length, complexity requirements, and password age.
2. **Set a Desktop Wallpaper:**
   * Navigate to: User Configuration > Policies > Administrative Templates > Desktop > Desktop.
   * Enable the policy **Desktop Wallpaper** and specify the image path.
3. **Disable USB Storage:**
   * Navigate to: Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access.
   * Enable the policy **Deny access to removable storage devices**.

**Step 8: Test and Validate the GPO**

1. On a domain-joined client machine, run gpupdate /force in Command Prompt to apply the GPO immediately.
2. Verify that the policy is applied:
   * For User Configuration: Log off and back on.
   * For Computer Configuration: Restart the machine.
3. Use the **Resultant Set of Policy (RSoP)** tool or run gpresult /r in Command Prompt to check which policies are applied.

**Step 9: Troubleshooting**

1. **GPO Not Applying:**
   * Ensure the GPO is linked to the correct domain/OU.
   * Verify that permissions on the GPO allow the intended users or computers to access it.
   * Check the network connection and domain membership of client machines.
2. **Conflicting GPOs:**
   * Use the **Group Policy Modeling Wizard** in the Group Policy Management Console to simulate policy application and resolve conflicts.