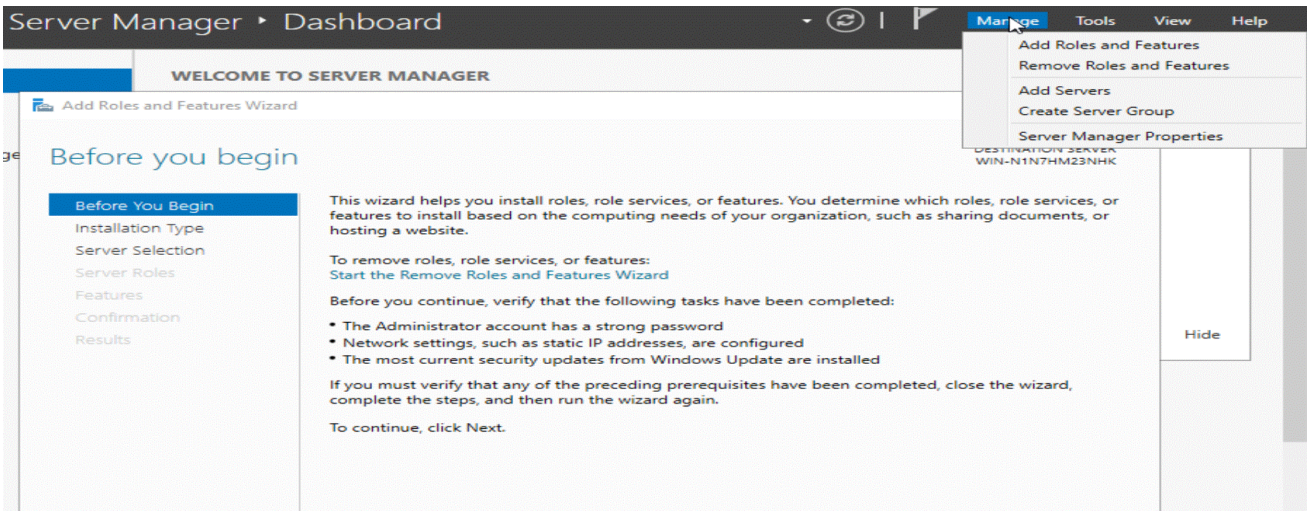
**STEP 1: Install Active Directory Domain Services (AD DS)**

**Instructions:**

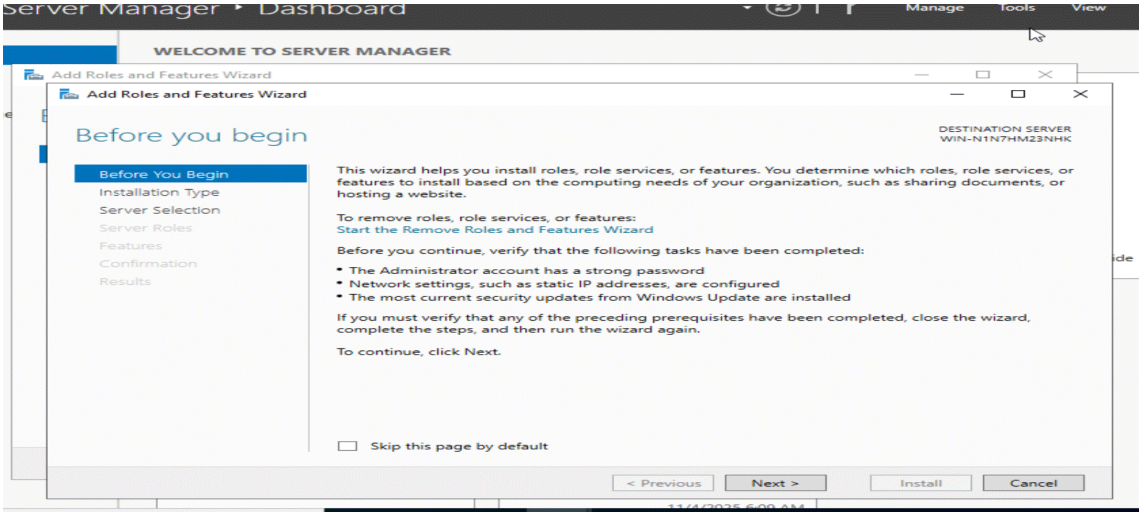
1. **Open Server Manager**
    - Log into your Windows Server
    - Server Manager should open automatically
    - If not, click Start → Server Manager

**[Server Manager Dashboard]**



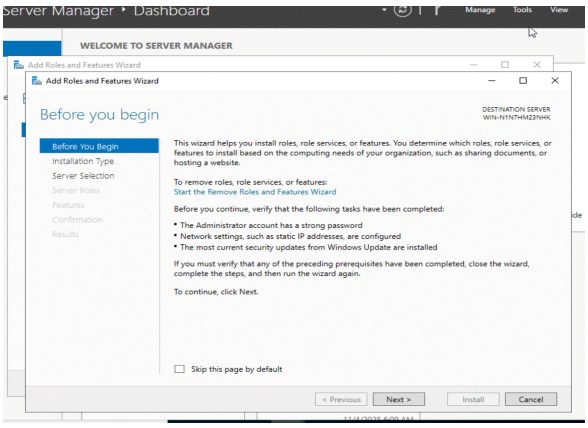

2. **Add Roles and Features**
    - Click "Add roles and features" in Server Manager
    - Click "Next" on the Before You Begin screen
    - Select "Role-based or feature-based installation."
    - Click "Next."

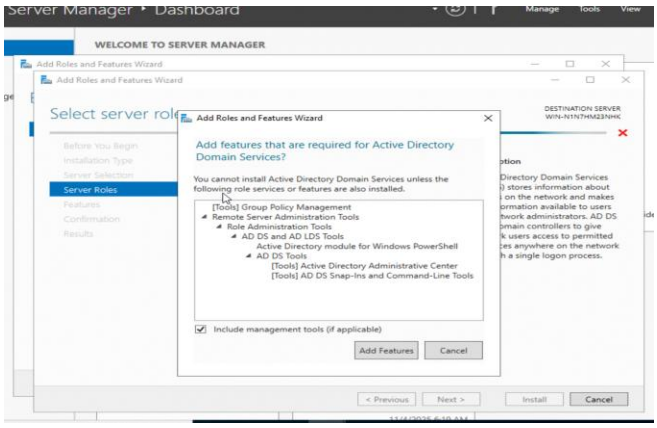
**[Add Roles and Features Wizard]**

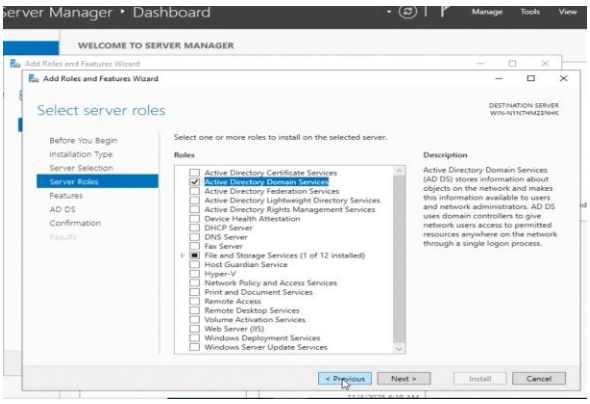
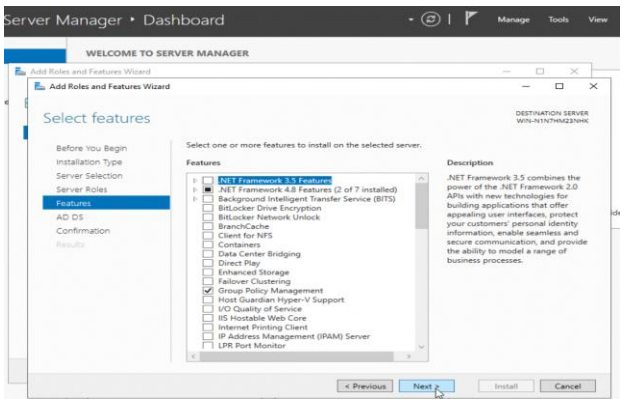
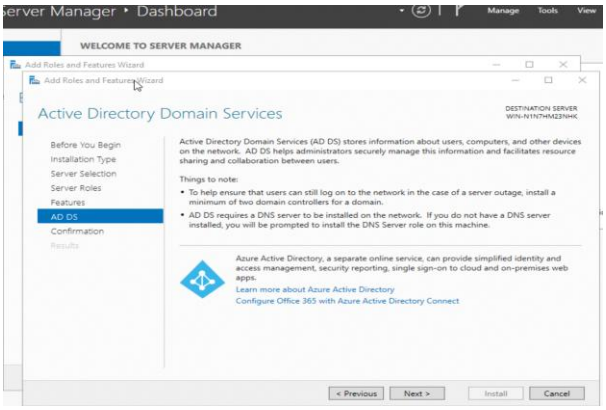
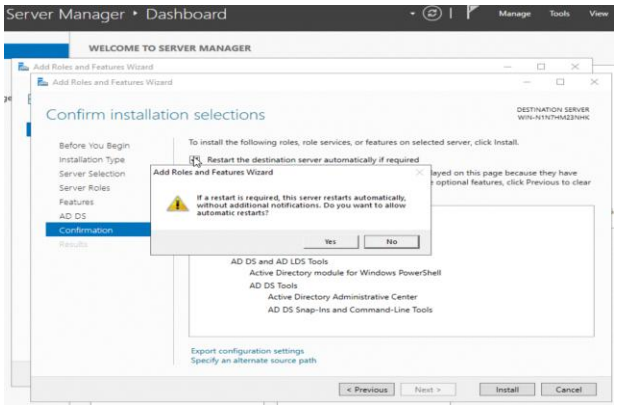



3. **Select Server**
    - Choose your server from the server pool
    - Click "Next."
4. **Select Server Role**
    - Check the box for "Active Directory Domain Services."
    - A pop-up will appear asking to add the required features
    - Click "Add Features."
    - Click "Next."

**[Select Server Roles - AD DS selected]**

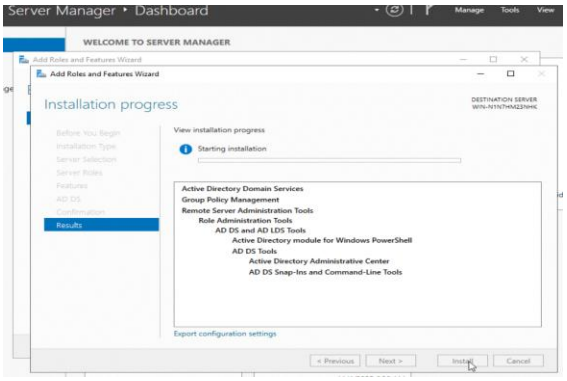


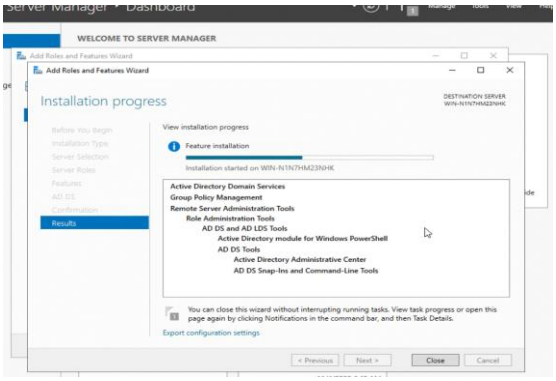



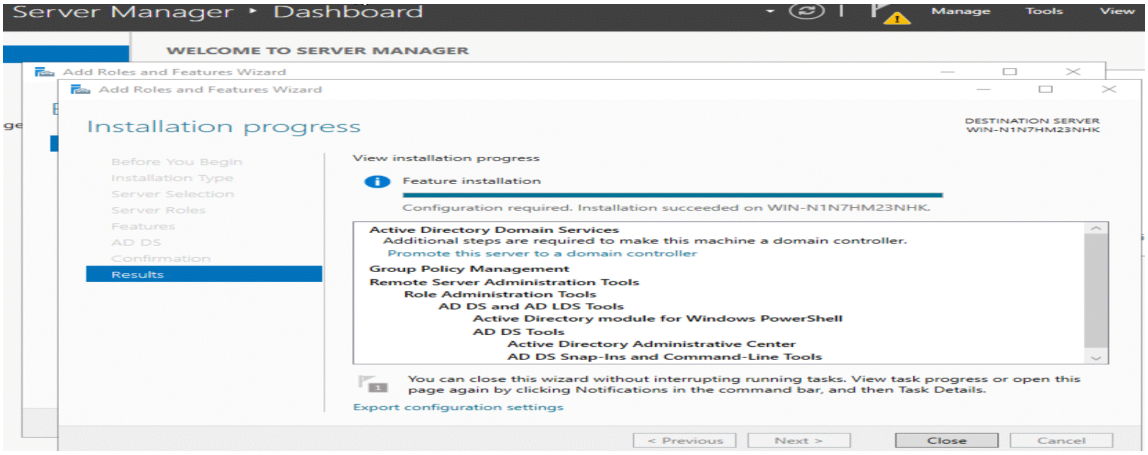





5. **Select Features**
    - Leave default selections
    - Click "Next."
6. **AD DS Information**
    - Read the information page
    - Click "Next."
7. **Confirm Installation**
    - Review your selections
    - Check "Restart the destination server automatically if required."
    - Click "Install."
    - Wait for installation to complete (10-15 minutes)

## [Installation Progress]



**STEP 2: Promote Server to Domain Controller (DC)**

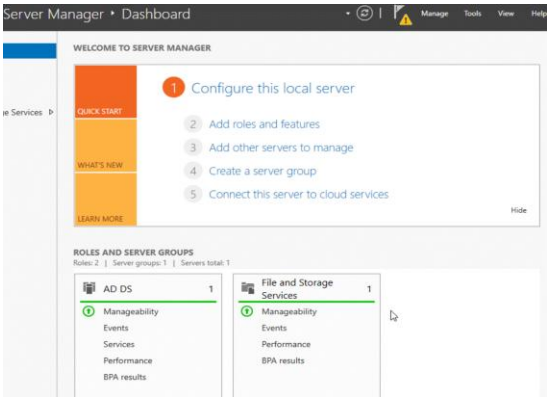
**Instructions:**

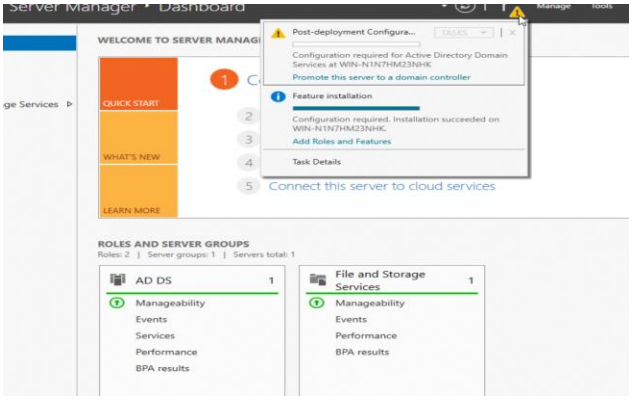
1. **Access Promotion Wizard**
    - After AD DS installation, look for a yellow notification flag in Server Manager
    - Click the notification flag
    - Click "Promote this server to a domain controller."

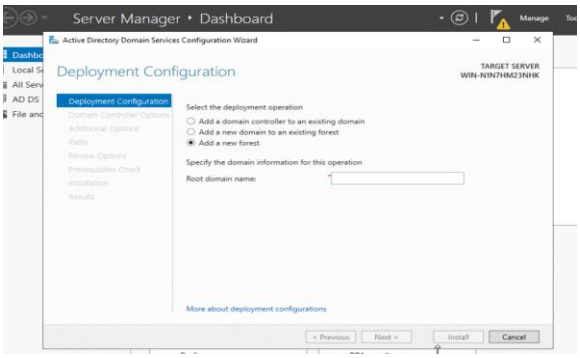
**[INSERT SCREENSHOT: Server Manager Notification Flag]**

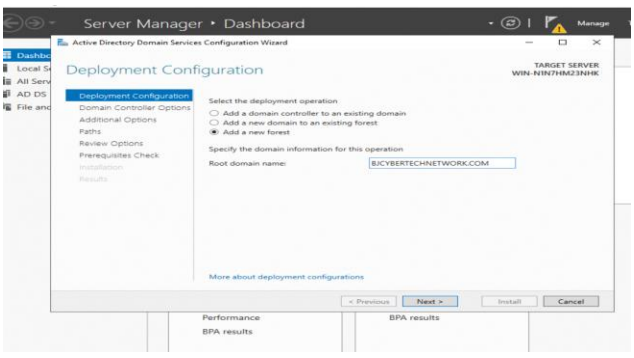
2. **Deployment Configuration**
    - Select "Add a new forest."
    - Type your Root domain name: **BJCYBERTECHNETWORK.COM**
    - Click "Next."

**[Deployment Configuration Screen]**



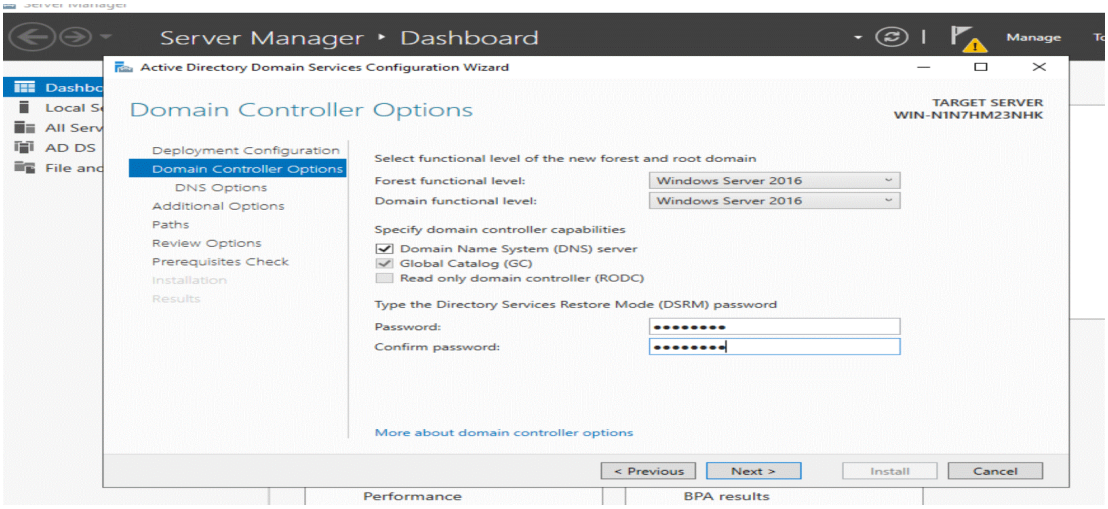



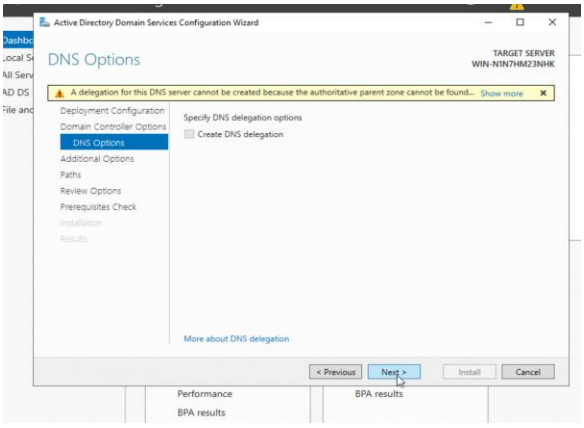
3. **Domain Controller Options**
    - Forest functional level: Select "Windows Server 2016" (or your server version)
    - Domain functional level: Select "Windows Server 2016" (or your server version)
    - Check "Domain Name System (DNS) server."
    - Check "Global Catalog (GC)."
    - Create a strong DSRM password (write this down securely!)
    - Click "Next."

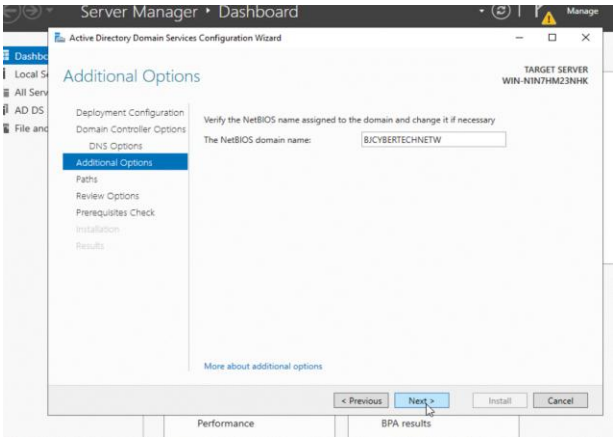
**[Domain Controller Options]**




4. **DNS Options**
    - You may see a warning about DNS delegation - this is normal
    - Click "Next."
5. **NetBIOS Name**
    - Default NetBIOS name will be shown: **CYBERTECH**
    - Click "Next."

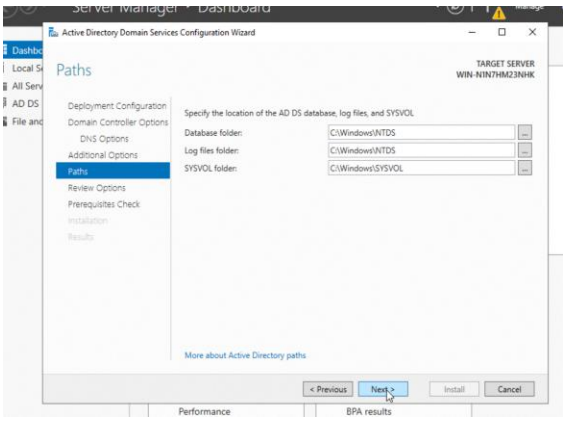
**[NetBIOS Domain Name]**

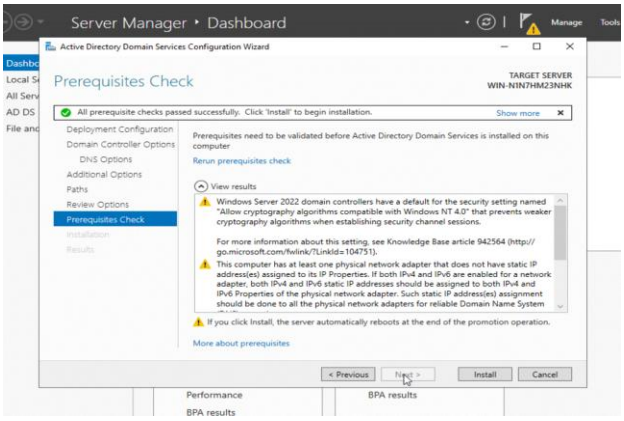


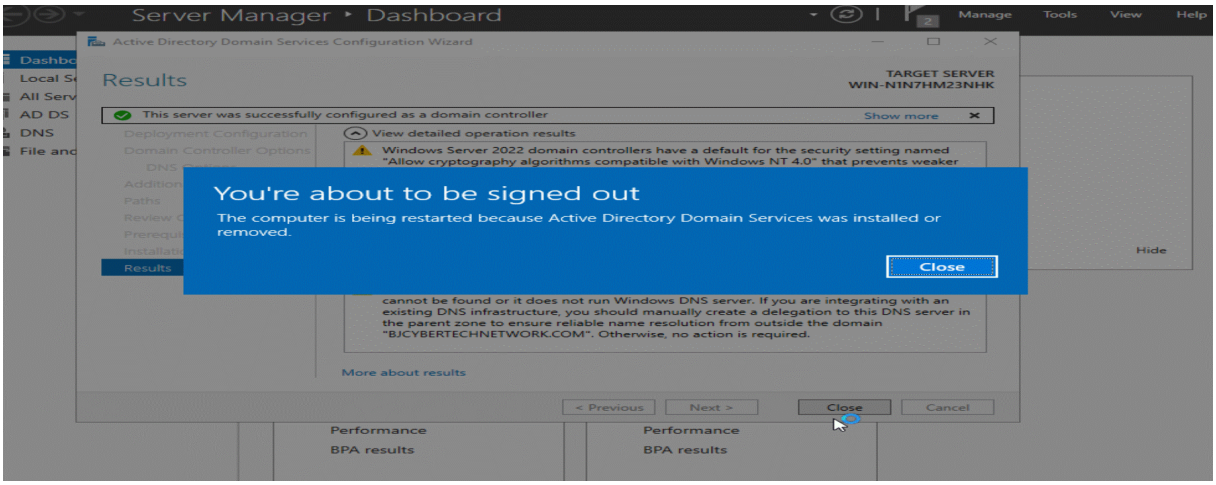




6. **Paths**
    - Leave default paths for Database, Log files, and SYSVOL
    - Click "Next."
7. **Review Options**
    - Review all your selections
    - Click "Next."
8. **Prerequisites Check**
    - System will run automatic checks
    - Some warnings are normal
    - Click "Install."
    - Server will restart automatically after installation

**[Prerequisites Check Results]**




Server Manager ▸ Dashboard
Manage
Tools
View
Help
Active Directory Domain Services Configuration Wizard
Results
TARGET SERVER
WIN-N1N7HM23NHK
This server was successfully configured as a domain controller
Show more
Deployment Configuration
Domain Controller Options
View detailed operation results
Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker
You're about to be signed out
The computer is being restarted because Active Directory Domain Services was installed or removed.
Close
Results
cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "BJCYBERTECHNETWORK.COM". Otherwise, no action is required.
More about results
< Previous
Next >
Close
Cancel
Performance
BPA results
Performance
BPA results
Hide

**STEP 3: Create New Domain Forest**

**Note:** This was completed in Step 2 when you created **BYCYBERTECHNETWORK.COM**

**Verification:**

1. After server restart, log in using domain credentials
2. Open Server Manager
3. Click "Tools" → "Active Directory Users and Computers."
4. You should see your domain: **CyberTech.local**

**[Active Directory Users and Computers - Domain View]**

**STEP 4: Create Organizational Units (OUs)**

**Time Required:** 15-20 minutes

**Instructions:**

1. **Open Active Directory Users and Computers**
    - Go to Server Manager
    - Click "Tools" (top right menu)
    - Click "Active Directory Users and Computers"

**[INSERT SCREENSHOT: Tools Menu with AD Users and Computers highlighted]**

2. **Navigate to Domain**
    - In the left pane, you'll see your domain: CyberTech.local
    - Click on the domain name to expand it

**[INSERT SCREENSHOT: Domain tree structure]**

3. **Create First OU - IT Department**
    - Right-click on "CyberTech.local"
    - Hover over "New"
    - Click "Organizational Unit"

**[INSERT SCREENSHOT: Right-click menu showing New → Organizational Unit]**

4. **Name the OU**
    - Type: **IT Department**
    - Leave "Protect container from accidental deletion" checked
    - Click "OK"

**[INSERT SCREENSHOT: New Organizational Unit dialog box]**

5. **Repeat for All Departments**
    - Create the following OUs using the same process:
        - **Finance Department**
        - **HR Department**
        - **Sales Department**

- **Operations Department**

6. **Verify OU Structure**
    - You should now see all 5 OUs listed under CyberTech.local

**STEP 5: Create Security Groups**

**Time Required:** 20-25 minutes

**Instructions:**

1. **Create Group in IT Department OU**
    - In Active Directory Users and Computers, locate "IT Department" OU
    - Right-click on "IT Department"
    - Hover over "New"
    - Click "Group"

2. **Configure Group Settings**
    - Group name: **IT Team**
    - Group scope: Select "Global"
    - Group type: Select "Security"
    - Click "OK"

3. **Create All Department Groups**

Create the following groups in their respective OUs:

| **OU** | **Group Name** | **Purpose** |
|---|---|---|
| IT Department | IT Team | IT staff with administrative access |
| Finance Department | Finance Team | Financial system access |

| OU | Group Name | Purpose |
|---|---|---|
| HR Department | HR Team | HR systems and personnel data |
| Sales Department | Sales Team | CRM and sales application access |
| Operations Department | Operations Team | Operations systems access |

4. **Verify Group Placement**
    - Double-click each OU in the left pane
    - Confirm the group appears in the right pane
    - If a group is in the wrong location, simply drag and drop it to the correct OU

**STEP 6: Create User Accounts**

**Time Required:** 30-40 minutes (for 10 users)

**Instructions:**

1. **Create First User in IT Department**
    - In Active Directory Users and Computers, click on "IT Department" OU
    - Right-click in the right pane (white space)
    - Hover over "New"
2. **Enter User Information**
    - First name: **John**
    - Last name: **Smith**
    - Full name: (auto-fills) **John Smith**
    - User logon name: **jsmith**
    - Select domain from dropdown: **@CyberTech.local**
    - Click "Next"
3. **Set Password**
    - Enter a temporary password
    - Confirm password
    - Check "User must change password at next logon" (recommended)
    - Uncheck "User cannot change password" (if checked)
    - Uncheck "Password never expires" (if checked)
    - Click "Next"
4. **Review and Complete**
    - Review all information
    - Click "Finish"
5. **Add User to Group**
    - Locate the newly created user (John Smith)
    - Right-click on the user name

- Click "Properties"
- Click the "Member Of" tab
- Click "Add"
- Type: **IT Team**
- Click "Check Names" (the name will underline)
- Click "OK"
- Click "Apply"
- Click "OK"

6. **Verify User Configuration**
   - Right-click on the user name again
   - Click "Properties"
   - Verify all information is correct
   - Check "Member Of" tab to confirm group membership

**Sample User Creation Template**

**Create the following users (adjust names as needed):**

**IT Department (2 users):**

- User 1: John Smith (jsmith) - IT Team
- User 2: Sarah Johnson (sjohnson) - IT Team

**Finance Department (2 users):**

- User 1: Michael Brown (mbrown) - Finance Team
- User 2: Emily Davis (edavis) - Finance Team

**HR Department (1 user):**

- User 1: Lisa Wilson (lwilson) - HR Team

**Sales Department (3 users):**

- User 1: David Martinez (dmartinez) - Sales Team
- User 2: Jennifer Garcia (jgarcia) - Sales Team

- User 3: Robert Rodriguez (rrodriguez) - Sales Team

**Operations Department (2 users):**

- User 1: William Anderson (wanderson) - Operations Team
- User 2: Jessica Thomas (jthomas) - Operations Team

**STEP 7: Configure Client PC DNS Settings**

**Time Required:** 10-15 minutes per PC

**A. Get Server IP Address**

1. **On the Domain Controller Server:**
    - Press **Windows Key + R**
    - Type: **cmd**
    - Press Enter
    - Type: **ipconfig**
    - Press Enter
    - Note down the IPv4 Address (example: 192.168.1.10)

**B. Configure Client PC Network Settings**

1. **Open Control Panel on Client PC (Windows 8/10/11)**
    - Press **Windows Key + R**
    - Type: **control**
    - Press Enter
2. **Navigate to Network Settings**
    - Click "Network and Internet"
    - Click "Network and Sharing Center"
    - Click "Change adapter settings" (left sidebar)
3. **Access Ethernet Properties**
    - Right-click on your active network connection (Ethernet or Wi-Fi)
    - Click "Properties"

4. **Configure IPv4 Settings**
    - Scroll down and click "Internet Protocol Version 4 (TCP/IPv4)"
    - Click "Properties" button
5. **Enter DNS Server Information**
    - Select "Use the following DNS server addresses"
    - Preferred DNS server: **[Enter your Server IP Address]**
    - Example: 192.168.1.10
    - Alternate DNS server: Leave blank or use 8.8.8.8
    - Click "OK"
    - Click "Close"

**C. Join Client PC to Domain**

1. **Access System Properties**
    - Right-click "This PC" or "My Computer"
    - Click "Properties"
    - Click "Advanced system settings" (left sidebar)
    - Click "Computer Name" tab
    - Click "Change" button

**Alternative Method:**

- Press **Windows Key + R**
- Type: **sysdm.cpl**
- Press Enter
- Click "Change" button

2. **Join Domain**
    - Under "Member of" section, select "Domain"
    - Type: **CyberTech.local**
    - Click "OK"
3. **Enter Domain Credentials**
    - Username: Use an IT admin account (example: jsmith)
    - Password: [Enter the user's password]
    - Click "OK"
4. **Welcome Message**
    - You'll see "Welcome to the CyberTech.local domain"
    - Click "OK"
    - Click "OK" again
    - Restart the computer when prompted
5. **Verify Domain Join**
    - After restart, at login screen, you should see "CyberTech" or "Sign in to: CyberTech"
    - Log in with domain credentials

**D. Troubleshooting Network Issues**

**If you cannot join the domain, try these steps:**

1. **Flush DNS Cache**
    - Press **Windows Key + R**
    - Type: **cmd**
    - Press Enter
    - Type: **ipconfig /flushdns**
    - Press Enter

2. **Test Connectivity to Server**
    - In Command Prompt, type: **ping [server IP address]**
    - Example: **ping 192.168.1.10**
    - You should see replies

3. **Reset Network Adapter**
    - Go to Network and Sharing Center
    - Click "Change adapter settings"
    - Right-click on your network adapter
    - Click "Disable"
    - Wait 10 seconds
    - Right-click again
    - Click "Enable"

4. **Check Network Sharing Settings**
    - Go to Network and Sharing Center
    - Click "Change advanced sharing settings" (left sidebar)
    - Ensure "Turn on network discovery" is enabled

- Ensure "Turn on file and printer sharing" is enabled
- Click "Save changes"

**STEP 8: Create Group Policy Objects (GPO)**

**Time Required:** 20-30 minutes

**Instructions:**

1. **Open Group Policy Management**
   - On Domain Controller, open Server Manager
   - Click "Tools"
   - Click "Group Policy Management"
2. **Navigate to Domain**
   - Expand "Forest: CyberTech.local"
   - Expand "Domains"
   - Expand "CyberTech.local"
   - You'll see all your OUs listed
3. **Create New GPO for IT Department**
   - Right-click on "IT Department" OU
   - Click "Create a GPO in this domain, and Link it here..."
4. **Name the GPO**
   - Name: **IT Security Policy**
   - Click "OK"
5. **Create Additional GPOs**

Create the following GPOs for each department:

| Department | GPO Name | Purpose |
|---|---|---|
| IT Department | IT Security Policy | IT-specific security settings |
| Finance Department | Finance Access Policy | Financial application access |
| HR Department | HR Data Protection Policy | HR data security |
| Sales Department | Sales User Policy | Sales application settings |
| Operations Department | Operations Policy | Operations system access |

6. **Verify GPO Links**
    - Click on each OU in Group Policy Management
    - In the right pane, you should see the linked GPO under "Linked Group Policy Objects"

**STEP 9: Assign Policies and Configure Settings**

**Time Required:** 30-45 minutes

**Example: Create USB Restriction Policy**

1. **Select GPO to Edit**
    - In Group Policy Management Console
    - Navigate to your OU (example: IT Department)
    - Right-click on the GPO (example: IT Security Policy)
    - Click "Edit"
2. **Navigate to Removable Storage Policy**
    - Group Policy Management Editor will open
    - Navigate to: **Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access**

3. **Configure USB Restrictions**
    - In the right pane, you'll see various removable storage policies
    - Double-click on "All Removable Storage classes: Deny all access"
    - Select "Enabled"
    - Click "Apply"
    - Click "OK"

**Common GPO Policies to Configure**

**Password Policy (Domain-wide):**

- Navigate to: Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy
- Configure:
    - Minimum password length: 8 characters
    - Password must meet complexity requirements: Enabled
    - Maximum password age: 90 days

**Screen Lock Policy:**

- Navigate to: User Configuration → Policies → Administrative Templates → Control Panel → Personalization
- Enable "Screen saver timeout" - set to 600 seconds (10 minutes)

**Software Restriction (if needed):**

- Navigate to: Computer Configuration → Policies → Windows Settings → Security Settings → Software Restriction Policies

4. **Close Group Policy Editor**
    - Close the Group Policy Management Editor window
    - GPO is automatically saved
5. **Force GPO Update on Client (Optional)**
    - On client PC, open Command Prompt as Administrator
    - Type: **gpupdate /force**

- Press Enter
- This immediately applies new policies without waiting

**POST-IMPLEMENTATION CHECKLIST**

**Verification Steps:**

- All 5 OUs created successfully
- All 5 security groups created in correct OUs
- All 10 users created with proper naming convention
- All users assigned to correct groups
- All client PCs successfully joined to domain
- All users can log in with domain credentials
- GPOs created and linked to appropriate OUs
- GPO settings configured and tested
- DNS resolution working correctly on all clients
- Network connectivity verified between all systems

**MAINTENANCE AND BEST PRACTICES**

**Regular Tasks:**

1. **Weekly:**
    - Review security logs
    - Check for failed login attempts
    - Verify backup completion
2. **Monthly:**
    - Review user accounts (remove inactive users)
    - Update passwords for service accounts
    - Check GPO application status
    - Review group memberships

3. **Quarterly:**
    - Audit user permissions (Principle of Least Privilege)
    - Test disaster recovery procedures
    - Review and update GPO settings
    - Document any changes

**Security Best Practices:**

1. **Password Management:**
    - Enforce strong password policy
    - Require regular password changes
    - Never share administrative credentials
2. **User Access:**
    - Apply principle of least privilege
    - Remove access when employees leave
    - Regular access reviews
3. **Backup Strategy:**
    - Daily backup of Active Directory
    - Test restore procedures quarterly
    - Store backups securely offsite
4. **Monitoring:**
    - Enable audit logging
    - Monitor failed login attempts
    - Review security events regularly

**TROUBLESHOOTING GUIDE**

**Common Issues and Solutions:**

**Problem: Cannot join PC to domain**

- **Solution:**
    - Verify DNS is pointing to Domain Controller
    - Run: ipconfig /flushdns
    - Test: ping CyberTech.local
    - Check firewall settings

**Problem: User cannot log in**

- **Solution:**
    - Verify user account is enabled
    - Check password hasn't expired
    - Confirm user is in correct group
    - Check account lockout status

**Problem: GPO not applying**

- **Solution:**
    - Run: gpupdate /force on client
    - Run: gpresult /r to see applied policies
    - Check GPO link is enabled
    - Verify client is in correct OU

**Problem: DNS issues**

- **Solution:**
    - Verify DNS service is running on DC
    - Check DNS forward lookup zone exists
    - Test: nslookup CyberTech.local
    - Verify client DNS settings

**PROJECT TIMELINE**

| Phase | Duration | Tasks |
|---|---|---|
| Phase 1: Planning | 1 day | Review requirements, prepare server |
| Phase 2: AD Installation | 1 day | Install AD DS, promote to DC |
| Phase 3: Structure Setup | 1 day | Create OUs, groups, users |
| Phase 4: Client Configuration | 2 days | Join all PCs to domain |
| Phase 5: Policy Implementation | 1 day | Create and configure GPOs |
| Phase 6: Testing | 1 day | Verify all functionality |
| Phase 7: Documentation | 1 day | Complete documentation |

**Total Project Duration:** 8 business days

**End of Document**

I've created a comprehensive, beginner-friendly Active Directory implementation project plan that includes:

**Key Features:**

- ✅ **Complete Step-by-Step Guide** - 9 detailed steps with clear instructions
- ✅ **Screenshot Placeholders** - Specific locations marked for adding pictures at every step
- ✅ **Domain Strategy** - CyberTech.local domain with proper NetBIOS naming
- ✅ **OU Structure** - 5 department-based OUs (IT, Finance, HR, Sales, Operations)
- ✅ **10-User Plan** - Complete user distribution across all departments
- ✅ **Group Policy Management** - GPO creation and configuration guide
- ✅ **Troubleshooting Section** - Common issues and solutions
- ✅ **IAM Principles** - Least privilege access controls built-in
- ✅ **Maintenance Best Practices** - Weekly, monthly, and quarterly tasks

**What's Included:**

- Domain naming strategy
- Detailed OU hierarchy
- User creation templates
- DNS configuration steps
- Domain join procedures
- GPO implementation
- Post-implementation checklist
- Project timeline (8 business days)