

## Module: 14- Identity with Windows Server

31. Explain the process of installing and configuring Hyper-V virtualization in Windows Server 2016.

Ans:

### Step 1: Check System Requirements

Ensure your server meets these requirements:

- 64-bit processor with virtualization support (Intel VT-x or AMD-V).
- At least 4 GB of RAM (8 GB recommended).
- Enable **Virtualization** in the BIOS.

### Step 2: Install the Hyper-V Role

1. Open **Server Manager**.
2. Click on **Manage > Add Roles and Features**.
3. Click **Next** until you reach the **Select Server Roles** page.
4. Check **Hyper-V**.
  - Click **Add Features** when prompted.
5. Click **Next**, then **Next** again.
6. Choose the network adapter to use for Hyper-V and click **Next**.
7. Click **Install**. Once done, restart the server.

### Step 3: Enable Virtualization in BIOS (if needed)

If Hyper-V doesn't work, go to **BIOS/UEFI** during startup and enable **Intel VT-x** or **AMD-V**.

### Step 4: Configure Hyper-V

1. Open **Hyper-V Manager**:
  - In **Server Manager**, click **Tools > Hyper-V Manager**.
2. Create a **Virtual Switch** for networking:
  - Click **Virtual Switch Manager** on the right.
  - Click **New virtual network switch > External**.
  - Click **Create Virtual Switch** and then **OK**.
3. Create a **Virtual Machine (VM)**:
  - In **Hyper-V Manager**, click **New > Virtual Machine**.
  - Follow the wizard:
    - Name your VM.
    - Set the amount of **memory** (RAM).
    - Choose **Generation 1** (or Generation 2 for UEFI systems).
    - Create a **virtual hard disk**.
    - Attach a **bootable ISO** to install an operating system.
  - Click **Finish**.
4. **Start the Virtual Machine**:

- Right-click on the VM in **Hyper-V Manager** and select **Start**.
  - Right-click again and click **Connect** to open the VM's console.
5. Install the **Operating System** on your VM like you would on a physical machine.

### Step 5: Manage Virtual Machines

- You can start, stop, or modify the settings of your VM from **Hyper-V Manager**.

32. How do you monitor server performance and manage event logs in Windows Server?

Ans:

## Part 1: Monitor Server Performance

### Step 1: Open Task Manager

1. Press Ctrl + Shift + Esc to open Task Manager.
2. In the Task Manager, click on the Performance tab.
3. Here, you can see CPU, memory, disk, and network usage in real time.

### Step 2: Use Resource Monitor

1. Right-click on the Start Menu and select Task Manager.
2. Click on the Performance tab.
3. At the bottom, click on Open Resource Monitor.
4. In Resource Monitor, you can see detailed information about CPU, Memory, Disk, and Network usage.

### Step 3: Use Performance Monitor (for detailed metrics)

1. Press Win + R, type perfmon, and press Enter.
2. In the Performance Monitor, click on Performance Monitor under Monitoring Tools.
3. You can add specific counters for CPU, memory, disk, and network by clicking on the green + icon.
4. Add the performance counters you want to track and click OK.

### Step 4: Set Up Alerts (Optional)

1. In Performance Monitor, right-click on Data Collector Sets > User Defined.
2. Click New > Data Collector Set to create a custom performance monitoring task.
3. Configure your alert settings, like when specific resource usage exceeds a certain threshold.

## Part 2: Manage Event Logs

### Step 1: Open Event Viewer

1. Press Win + R, type eventvwr.msc, and press Enter.

2. This opens the Event Viewer.

#### Step 2: View Event Logs

1. In the Event Viewer, expand Windows Logs in the left pane.
2. You'll see Application, Security, System, and Setup logs.
3. Click on each log type to view events related to that category.
  - Application logs: Events related to applications.
  - Security logs: Security-related events (e.g., login attempts).
  - System logs: Events related to system operations (e.g., hardware or OS issues).

#### Step 3: Filter Event Logs

1. In the Event Viewer, select a log (e.g., System).
2. On the right, click Filter Current Log.
3. Set the filter criteria (e.g., specific event IDs or date ranges).
4. Click OK to apply the filter.

#### Step 4: Create Custom Views (for specific events)

1. In the Event Viewer, click on Custom Views in the left pane.
2. Right-click on Custom Views and select Create Custom View.
3. Define your filters (e.g., log type, event ID, severity) and click OK.
4. Give your custom view a name and click OK to save it.

#### Step 5: Export Event Logs (Optional)

1. In Event Viewer, right-click on a log (e.g., System) and select Save All Events As.
2. Choose the location to save the log file and select the file format (usually .evtx).
3. Click Save to export the log.

33. Describe the different types of storage options available in Windows Server.

Ans:

#### Step 1: Local Storage

- **What it is:** Hard drives or SSDs directly connected to the server.
- **Details:** Simple and cheap, like an internal disk or USB drive.
- **Use:** Small setups with basic needs.

#### Step 2: RAID

- **What it is:** Combines multiple disks for speed or safety.
- **Types:**
  1. RAID 0: Faster, no backup.
  2. RAID 1: Mirrors data for safety.
  3. RAID 5: Mixes speed and backup (needs 3+ disks).

- **Use:** Better performance or protection.

### Step 3: Storage Spaces

- **What it is:** Groups disks into a virtual pool.
- **Details:** Create flexible storage with options like mirroring or parity.
- **Use:** Custom storage with redundancy.

### Step 4: Storage Spaces Direct

- **What it is:** Storage Spaces for multiple servers (clusters).
- **Details:** Shares storage across servers for high availability.
- **Use:** Big, scalable systems.

### Step 5: Network Storage (NAS/SAN)

- **What it is:** Storage over a network.
- **Details:**
  - NAS: Shared folders via SMB.
  - SAN: Fast, dedicated network (iSCSI or Fibre Channel).
- **Use:** Centralized or enterprise storage.

### Step 6: File Systems

- **What it is:** How data is organized.
- **Options:**
  1. NTFS: Standard, secure.
  2. ReFS: Newer, resilient.
- **Use:** Pick NTFS for most cases, ReFS for advanced needs.

34. What is the role of File Server in Windows Server, and how do you configure it?

Ans:

#### Step 1: Understand the Role of a File Server

A **File Server** in Windows Server is used to store, manage, and share files across a network. It allows multiple users to access files from different devices, centralizes file storage, and controls who can read, write, or modify files. The main benefits are **easy file sharing**, **enhanced security**, and **simplified backups**.

#### Step 2: Prerequisites

Before setting up a file server, ensure you have:

- A **Windows Server** installed (such as Windows Server 2019 or 2022).
- **Network connectivity** to allow users to access the server.
- **Administrator access** to configure the file server.

- **Storage:** Set up disk drives or volumes (using NTFS) to store the files that will be shared.

### Step 3: Install the File Server Role

1. Open **Server Manager** from the Start menu.
2. Click **Manage > Add Roles and Features** to start the wizard.
3. In the wizard, click **Next** until you reach the **Server Roles** page.
4. Expand **File and Storage Services > File and iSCSI Services**.
5. Check the **File Server** box, then click **Next** and select **Install**.
6. Once installation is complete, the **File Server** role will be added.

### Step 4: Configure Shared Folders

1. In **Server Manager**, go to **File and Storage Services > Shares**.
2. Click **Tasks > New Share** to begin creating a new shared folder.
3. Choose a share type, such as **SMB Share - Quick** for basic file sharing.
4. Select the folder location (e.g., **C:\Shares**) or create a new one.
5. Set a **share name** (e.g., "TeamFiles") and provide a description.
6. Click **Next** and configure **permissions** (e.g., grant "Everyone" read-only or assign specific users full access).
7. Complete the wizard, and the shared folder is now accessible across the network.

### Step 5: Set Permissions

1. Right-click the shared folder and select **Properties**.
2. Go to the **Security** tab.
3. Add users or groups, and set specific permissions (e.g., **Read, Write, or Full Control**).
4. Ensure that the **share permissions** set earlier align with the **NTFS permissions** to avoid conflicting access rules.

### Step 6: Access the File Server

1. On a **client PC**, open **File Explorer** and type the server path: `\\ServerName\ShareName` (e.g., `\\Server1\TeamFiles`).
2. Test access to ensure users can open, edit, or save files based on their assigned permissions.

35. Explain the process of implementing and managing Distributed File System (DFS) in Windows Server 2016.

Ans:

#### Step 1: Install DFS Role

1. Open **Server Manager**.
2. Click **Manage > Add Roles and Features**.
3. In the wizard, click **Next** until you reach **Server Roles**.
4. Expand **File and Storage Services > DFS Namespaces and DFS Replication**.
5. Check both **DFS Namespaces** and **DFS Replication**, then click **Next** and **Install**.

### Step 2: Configure DFS Namespace

1. Open Server Manager > Tools > DFS Management.
2. Right-click Namespaces > New Namespace.
3. Select a server for the namespace and click Next.
4. Choose the namespace type (e.g., Domain-based) and click Next.
5. Name your namespace (e.g., CompanyFiles) and click Next > Create.

### Step 3: Add Folders to the DFS Namespace

1. In DFS Management, right-click the namespace you created.
2. Click New Folder and enter the folder name (e.g., HRFiles).
3. Add folder targets (e.g., network paths to shared folders on different servers).
4. Click OK to finish adding the folder.

### Step 4: Configure DFS Replication

1. In DFS Management, click on Replication > New Replication Group.
2. Choose the replication group type (e.g., Multipurpose replication group).
3. Add servers to replicate folders and define the replication folder paths.
4. Set replication schedules and bandwidth limits, then click Next > Create.

### Step 5: Monitor DFS Health

1. In DFS Management, under Replication, right-click the replication group.
2. Click Show Replication Status to monitor the health of replication.
3. Use Event Viewer or Performance Monitor to track any replication issues.

### Step 6: Manage DFS Permissions

1. Right-click a DFS folder in the DFS Management console.
2. Click Properties > Security tab.
3. Set NTFS and share permissions to control access.

36. Discuss the built-in backup and recovery options available in Windows Server 2016 or 2019.

Ans:

### Step 1: Install Windows Server Backup Feature

1. Open **Server Manager**.
2. Click **Manage > Add Roles and Features**.
3. In the wizard, click **Next** until you reach **Features**.
4. Check **Windows Server Backup** and click **Next > Install**.

### Step 2: Open Windows Server Backup

1. After installation, open **Server Manager**.
2. Click **Tools > Windows Server Backup**.

### Step 3: Create a Backup

1. In **Windows Server Backup**, click **Backup Once** or **Backup Schedule**.
2. Choose **Custom** or **Full Server** backup.
  - **Full Server**: Backs up everything, including system files.
  - **Custom**: Select specific files or folders to back up.
3. Set the destination (e.g., external hard drive, network share).
4. Click **Backup** to start the process.

### Step 4: Schedule Regular Backups

1. In **Windows Server Backup**, click **Backup Schedule**.
2. Follow the wizard to set the frequency (daily, weekly, etc.) and backup type.
3. Select what to back up (e.g., full server or custom).
4. Choose a backup destination and finish the setup.

### Step 5: Recover Files or System

1. In **Windows Server Backup**, click **Recover**.
2. Select the **Recovery type** (e.g., **Files, Applications**, or **Full Server**).
3. Choose the location of the backup (e.g., from an external drive or network share).
4. Select the data you want to restore and follow the prompts to recover.

### Step 6: Use System Image Recovery (for Full System Restore)

1. Boot the server from **Windows Server installation media** or **Recovery Drive**.
2. Select **Repair your computer > Troubleshoot > Advanced Options > System Image Recovery**.
3. Follow the steps to restore the system from a previous backup image.

37. How do you configure Windows Server Backup to back up critical data?

Ans:

### Step 1: Install Windows Server Backup

1. Open **Server Manager**.
2. Click **Manage > Add Roles and Features**.
3. Check **Windows Server Backup** under **Features**.
4. Click **Install**.

### Step 2: Open Windows Server Backup

1. Open **Server Manager**.
2. Click **Tools > Windows Server Backup**.

### Step 3: Start a Custom Backup

1. In **Windows Server Backup**, click **Backup Once**.
2. Choose **Custom** and click **Next**.

### Step 4: Select Critical Data

1. Click **Add Items**.
2. Select the folders/drives with critical data.
3. Click **OK**, then **Next**.

### Step 5: Choose Backup Location

1. Select where to save the backup (external drive or network share).
2. Click **Next**.

### Step 6: Run the Backup

1. Click **Backup** to start the backup process.

38. Explain the steps for restoring files and folders using Windows Server Backup.

Ans:

**Step 1: Open Windows Server Backup:** Go to **Server Manager > Tools > Windows Server Backup**.

**Step 2: Start Recovery:** Click **Recover** in the right panel.

**Step 3: Choose Backup Location:** Select where the backup is stored (local drive or network) and click **Next**.

**Step 4: Select Backup to Restore:** Pick the backup date/time and click **Next**.

**Step 5: Choose Files/Folders to Restore:** Select **Files and Folders**, then click **Next**.

**Step 6: Choose Restore Location:** Choose to restore files to their **original** or **new location**.

**Step 7: Start Recovery:** Click **Recover** and wait for the process to complete.



39. What are some common troubleshooting techniques for Windows Server startup issues?

Ans:

**Step 1: Check Hardware**

- Ensure all cables, power supplies, and hardware components are connected properly.

**Step 2: Boot into Safe Mode**

- Restart the server and press **F8** (or **Shift + F8** for newer versions) and choose **Safe Mode**.

**Step 3: Use Last Known Good Configuration**

- Press **F8** during startup and select **Last Known Good Configuration** to restore a working state.

**Step 4: Check Boot Logs**

- Press **F8**, select **Enable Boot Logging**, and check the **ntbtlog.txt** for errors.

**Step 5: Use Startup Repair**

1. Boot from Windows Server installation media.
2. Choose **Repair your computer > Troubleshoot > Startup Repair**.

**Step 6: Check Event Viewer**

- Use **Event Viewer** to look for errors under **System** or **Application** logs.

**Step 7: Perform System Restore**

1. Boot from Windows installation media.
2. Select **Repair your computer > Troubleshoot > System Restore**.

**Step 8: Run CHKDSK**

1. Boot from installation media or into **Safe Mode**.
2. Open **Command Prompt** and run **chkdsk /f** to fix disk errors.

**Step 9: Reset BIOS/UEFI**

- Reset BIOS/UEFI settings to default if the boot order is misconfigured.

**Step 10: Reinstall Windows Server**

- If other steps fail, back up data and reinstall Windows Server.

40. How do you troubleshoot network connectivity problems in Windows Server?

Ans:

#### **Step 1: Check Physical Connections**

- Ensure cables are connected and network lights are on.

#### **Step 2: Verify IP Configuration**

1. Open **Command Prompt**.
2. Type ipconfig and check the **IP address**, **Subnet mask**, and **Gateway**.

#### **Step 3: Ping the Server**

- Type ping 127.0.0.1 to test the loopback, then ping <server IP>.

#### **Step 4: Ping the Default Gateway**

- Type ping <gateway IP> to check connectivity to the local network.

#### **Step 5: Check DNS**

- Type nslookup in **Command Prompt** to verify DNS server response.

#### **Step 6: Disable Firewall Temporarily**

- Temporarily disable Windows Firewall and test the connection.

#### **Step 7: Check for Duplicate IPs**

- Run arp -a to look for duplicate IP addresses on the network.

#### **Step 8: Verify Network Adapter**

- Check **Device Manager** for any issues with the network adapter.

#### **Step 9: Restart Network Services**

- Run netsh int ip reset and netsh winsock reset in **Command Prompt**.

#### **Step 10: Check Router/Switch**

- Verify that routers or switches are properly configured and working.

41. Discuss common Active Directory-related issues and their troubleshooting steps.

Ans:

**Step 1: Check Domain Controller Health**

- Open **Command Prompt** and run: dcdiag.

**Step 2: Verify DNS Configuration**

- Run nslookup to check DNS settings and ensure proper DNS resolution.

**Step 3: Check Active Directory Replication**

- Run repadmin /replsummary to check replication status.

**Step 4: Ensure Time Synchronization**

- Run w32tm /query /status to ensure Domain Controllers are synchronized.

**Step 5: Verify User Account Issues**

- Check **Active Directory Users and Computers** for disabled accounts or password issues.

**Step 6: Check Event Logs**

- Open **Event Viewer** and look for errors in **Directory Service** and **DNS Server** logs.

**Step 7: Run Active Directory Repair (if needed)**

- Run ntdsutil in **Command Prompt** to repair the Active Directory database.

**Step 8: Check Group Policy**

- Run gpresult /r to verify if Group Policies are applied correctly.

**Step 9: Test Connectivity Between Domain Controllers**

- Use **ping** or **telnet** to test communication on port 389 (LDAP).

**Step 10: Restart Active Directory Services**

- Restart **Active Directory Domain Services** from **Services.msc**.

42. Explain how to troubleshoot performance problems on Windows Server 2016 or 2019.

Ans:

**Step 1: Check Task Manager**

- Open **Task Manager** (Ctrl + Shift + Esc) and check **CPU**, **Memory**, and **Disk** usage.

**Step 2: Identify High Resource Usage**

- In **Task Manager**, sort by **CPU** or **Memory** to find high-usage processes.

**Step 3: Check Disk Space**

- Open **File Explorer** and ensure there's enough free space on the system drive.

**Step 4: Use Performance Monitor**

- Press **Win + R**, type perfmon, and monitor system performance.

**Step 5: Review Event Viewer**

- Open **Event Viewer** and check for errors in **System** or **Application** logs.

**Step 6: Update Drivers and Windows**

- Update device drivers in **Device Manager** and install any **Windows Updates**.

**Step 7: Check Virtual Memory Settings**

- Go to **System Properties > Performance Settings > Virtual Memory** and ensure it's set correctly.

**Step 8: Disable Unnecessary Startup Programs**

- In **Task Manager**, go to **Startup** and disable unnecessary apps.

**Step 9: Run Disk Cleanup**

- Right-click **C:** drive > **Properties > Disk Cleanup** to clear unnecessary files.