

**Hardware Networking**

**Identity with Windows Server**

**SUBMITTED TO**

**KAMLESH SHUKLA SIR**

**SUBMITTED BY**

**MANAV BANDHANIA**

**1. Installing and Configuring Hyper-V in Windows Server 2016**

**Step 1: Check System Requirements**

Before installing Hyper-V, ensure the following:

* **64-bit processor with Second Level Address Translation (SLAT)**
* **CPU virtualization support** (Intel VT-x or AMD-V, enabled in BIOS/UEFI)
* **At least 4GB RAM** (More recommended for running multiple VMs)
* **Windows Server 2016 Standard or Datacenter Edition**

**Step 2: Install Hyper-V Role**

1. **Open Server Manager** and click **Manage > Add Roles and Features**.
2. Select **Role-based or Feature-based Installation**.
3. Choose the local server and click **Next**.
4. Check **Hyper-V** and click **Next**.
5. Select **Network Adapter** for virtual switch configuration.
6. Enable **Live Migration** (optional).
7. Confirm installation and **Restart** the server.

**Step 3: Configure Hyper-V**

* **Create a Virtual Switch**
  1. Open **Hyper-V Manager**.
  2. Click **Virtual Switch Manager** > **New Virtual Switch**.
  3. Choose **External, Internal, or Private** switch type.
  4. Assign a name and apply settings.
* **Create a Virtual Machine (VM)**
  1. In **Hyper-V Manager**, select **New > Virtual Machine**.
  2. Configure **VM name, memory, and networking**.
  3. Attach a **virtual hard disk (VHD)**.
  4. Choose installation media (ISO, PXE, etc.).
  5. Complete the setup and **Start the VM**.

**2. Monitoring Server Performance and Managing Event Logs**

**Performance Monitoring Tools**

1. **Task Manager** – Monitor real-time CPU, memory, disk, and network usage.
2. **Performance Monitor (perfmon.msc)** – Add counters for CPU, RAM, disk I/O, network.
3. **Resource Monitor (resmon.exe)** – Detailed analysis of system resources.

**Event Logs Management**

1. Open **Event Viewer (eventvwr.msc)**.
2. Check **Windows Logs** for System, Security, Application events.
3. Use **Custom Views** to filter important events.
4. Enable **Event Forwarding** for centralized logging.
5. Set **Task Scheduler** to trigger actions based on specific logs.

**3. Storage Options in Windows Server**

1. **Local Storage** – Direct-attached HDDs or SSDs.
2. **Storage Spaces** – Software-defined storage using multiple disks.
3. **SAN (Storage Area Network)** – High-speed block-level storage.
4. **NAS (Network Attached Storage)** – File-based storage over a network.
5. **ReFS (Resilient File System)** – Optimized for large-scale data storage.
6. **iSCSI Storage** – Block-level storage over IP networks.
7. **Cloud Storage** – Integration with Azure Backup and OneDrive.

**4. Role of File Server in Windows Server & Its Configuration**

**What is a File Server?**

A **File Server** is a role in Windows Server that allows users and applications to **store, share, and manage files** over a network. It provides centralized access control, storage management, and data security.

**Key Features of a File Server:**

* Centralized storage and access control
* File sharing over SMB (Windows) and NFS (Linux)
* NTFS and Share-level permissions
* Quotas and file screening using File Server Resource Manager (FSRM)
* Distributed File System (DFS) for redundancy

**Steps to Configure a File Server in Windows Server 2016/2019**

**Step 1: Install the File Server Role**

1. Open **Server Manager**.
2. Click **Manage** > **Add Roles and Features**.
3. Select **Role-based or Feature-based Installation**.
4. Choose the server where you want to install the role.
5. Select **File and Storage Services** > **File Server**.
6. Click **Next** and install the role.

**Step 2: Create and Share a Folder**

1. Open **File Explorer** and navigate to a drive (e.g., C:\Shares).
2. Right-click > **New Folder** (e.g., CompanyFiles).
3. Right-click the folder > **Properties** > **Sharing** tab.
4. Click **Advanced Sharing** > **Check "Share this folder"**.
5. Click **Permissions** > Add **users or groups** > Assign **Read/Write permissions**.
6. Click **Apply** and **OK**.

**Step 3: Configure NTFS Permissions**

1. Go to the folder's **Properties** > **Security** tab.
2. Click **Edit** > **Add Users or Groups**.
3. Assign **permissions** (Full Control, Modify, Read & Execute).
4. Click **Apply** and **OK**.

**Step 4: Configure File Server Resource Manager (FSRM) (Optional)**

FSRM helps manage storage with quotas and file screening.

1. Open **Server Manager** > **Add Roles and Features**.
2. Select **File Server Resource Manager (FSRM)** under **File and Storage Services**.
3. Configure **Quota Management** to limit storage per user.
4. Use **File Screening** to restrict file types (e.g., block .exe uploads).

**5. Implementing and Managing Distributed File System (DFS) in Windows Server 2016**

DFS allows administrators to organize shared folders from multiple servers into a **single namespace**, making it easier for users to access files without knowing the exact server location.

**Types of DFS:**

1. **DFS Namespace** – Creates a virtual folder structure (\\Domain\DFSRoot).
2. **DFS Replication** – Synchronizes files across multiple servers for redundancy.

**Step-by-Step DFS Configuration**

**Step 1: Install DFS Roles**

1. Open **Server Manager** > **Manage** > **Add Roles and Features**.
2. Select **DFS Namespaces** and **DFS Replication**.
3. Click **Next** and install the roles.

**Step 2: Create a DFS Namespace**

1. Open **DFS Management** (dfsmgmt.msc).
2. Right-click **Namespaces** > **New Namespace**.
3. Select the **Server** that will host the namespace.
4. Name the namespace (e.g., CompanyShares).
5. Choose **Domain-based** or **Standalone**.
6. Click **Create** to finish.

**Step 3: Add Shared Folders to DFS**

1. Open **DFS Management** > Select **Namespace**.
2. Right-click **Namespace** > **New Folder**.
3. Provide a name (e.g., HRFiles) and add a shared folder path (\\Server1\HR).
4. Repeat for additional shared folders.

**Step 4: Configure DFS Replication**

1. Open **DFS Management** > **Replication**.
2. Click **New Replication Group** > Choose **Multipurpose or Hub & Spoke**.
3. Select **Servers to replicate** files across.
4. Define **Replication Schedule & Bandwidth**.
5. Click **Create** and start the replication.

**6. Built-in Backup and Recovery Options in Windows Server 2016/2019**

**Windows Server Backup (WSB) Features:**

* Supports **full system, volume, file, and system state backup**
* Scheduled and manual backups
* Backup to **local disk, network, or cloud (Azure Backup)**
* Supports **Volume Shadow Copy**

**Other Backup & Recovery Options:**

1. **Active Directory Recycle Bin** – Restores deleted AD objects.
2. **System Restore & System Image Backup** – Restores entire OS.
3. **Azure Backup** – Cloud-based backup solution.
4. **Volume Shadow Copy (VSS)** – Creates point-in-time snapshots.

**7. Configuring Windows Server Backup to Back Up Critical Data**

**Windows Server Backup (WSB)** is a built-in feature that allows full and incremental backups of data, system states, and entire servers. It supports **backup to local disks, network shares, or external storage**.

**Step 1: Install Windows Server Backup Feature**

If not installed, follow these steps:

1. Open **Server Manager** > Click **Manage** > **Add Roles and Features**.
2. Select **Role-based or Feature-based Installation**.
3. Under **Features**, check **Windows Server Backup**.
4. Click **Next** and **Install**.

**Step 2: Open Windows Server Backup**

1. Press **Win + R**, type wbadmin.msc, and hit **Enter**.
2. In the **Windows Server Backup console**, select **Local Backup**.

**Step 3: Configure Backup Schedule**

1. Click **Backup Schedule** in the right panel.
2. Choose **Full Server** or **Custom Backup** (to back up specific drives, folders, or system states).
3. Select the **backup destination**:
   * Local disk
   * Network share (UNC path, e.g., \\BackupServer\Backups)
   * External drive
4. Set **backup frequency**: Daily, Weekly, or Custom.
5. Click **Finish** to apply the backup schedule.

**Step 4: Run an Immediate Backup (Optional)**

1. Click **Backup Once** from the right panel.
2. Choose **"Scheduled settings" or "Different options"**.
3. Select **Backup Destination** and click **Backup**.

**Step 5: Verify Backup Status**

1. Open **Windows Server Backup**.
2. Click **Backup History** to check past backups.
3. Check **Event Viewer** (eventvwr.msc) under **Applications and Services Logs > Microsoft > Windows > Backup** for any issues.

**8. Restoring Files and Folders Using Windows Server Backup**

**Step 1: Open Windows Server Backup**

1. Press **Win + R**, type wbadmin.msc, and hit **Enter**.
2. Click **Recover** in the right panel.

**Step 2: Select Backup Source**

* If backup is stored locally, select **"This Server"**.
* If backup is on another location, choose **"Another location"** and browse to it.

**Step 3: Select Recovery Type**

Choose from the following options:

* **Files and Folders** – Restore specific files.
* **Volumes** – Restore an entire drive.
* **System State** – Restore AD, registry, system services.
* **Full Server Recovery** – Restore the entire OS and data.

**Step 4: Choose the Backup Date & Files**

1. Select the **backup date and time** from the list.
2. Choose files or folders to restore.
3. Specify **Restore Location**:
   * **Original Location** (overwrites existing files).
   * **Alternate Location** (new folder or drive).

**Step 5: Begin Recovery**

* Click **Recover** to start the restore process.
* Check the **progress bar** and logs for errors.
* Use **Event Viewer** to verify successful restoration.

**9. Troubleshooting Windows Server Startup Issues**

When a Windows Server fails to start, it can be due to **corrupt system files, driver issues, or disk failures**.

**Step 1: Boot into Safe Mode**

1. Restart the server.
2. Press **F8 or Shift + F8** before the Windows logo appears.
3. Select **Safe Mode with Networking**.
4. If the system boots successfully, check **Event Viewer** for startup errors.

**Step 2: Use Windows Recovery Environment (WinRE)**

1. Insert **Windows Server installation media** and boot from it.
2. Select **Repair your Computer** > **Troubleshoot**.
3. Choose **Startup Repair** to fix common boot issues.

**Step 3: Repair Boot Configuration Data (BCD)**

1. Open **Command Prompt** in recovery mode.
2. Run these commands:
3. bootrec /fixmbr
4. bootrec /fixboot
5. bootrec /scanos
6. bootrec /rebuildbcd
7. Restart the server and check if the issue is resolved.

**Step 4: Restore from a System Image Backup**

1. Boot into **WinRE**.
2. Select **System Image Recovery**.
3. Choose a recent backup and restore the system.

**10. Troubleshooting Network Connectivity Issues in Windows Server**

**Common Network Issues:**

* No internet or LAN access
* Cannot communicate with other servers
* Incorrect DNS or IP settings
* Windows Firewall blocking connections

**Step 1: Check Network Configuration**

1. Open **Command Prompt** (cmd).
2. Run:
3. ipconfig /all
   * Verify the **IP address, Subnet Mask, and Default Gateway**.

**Step 2: Test Network Connectivity**

* Run:
* ping 8.8.8.8
  + If it fails, there's no internet connectivity.
* tracert google.com
  + Identifies where packets are getting dropped.

**Step 3: Restart Network Services**

1. Open **Command Prompt** as Administrator.
2. Run:
3. net stop netlogon
4. net start netlogon
5. Restart **DNS and DHCP services** in **services.msc**.

**Step 4: Reset Network Stack**

If the issue persists, reset TCP/IP settings:

netsh int ip reset

netsh winsock reset

ipconfig /flushdns

Reboot the server.

**11. Common Active Directory Issues and Troubleshooting**

**Issue 1: AD Replication Fails**

Run:

repadmin /showrepl

repadmin /replsummary

If replication fails, check network settings and **restart AD services**.

**Issue 2: Group Policies Not Applying**

Check policy results with:

gpresult /r

If Group Policy fails, run:

gpupdate /force

**Issue 3: User Login Failures**

* Check **Account Lockout Policy** in **Group Policy Editor**.
* Verify **Kerberos authentication** with:
* klist tickets

**Issue 4: DNS Misconfiguration**

Check AD DNS records:

nslookup domain.local

dcdiag /test:DNS

Ensure the correct DNS settings in **NIC properties**.

**12. Troubleshooting Performance Problems on Windows Server**

**Step 1: Identify Performance Bottlenecks**

1. Open **Task Manager** (Ctrl + Shift + Esc).
2. Check **CPU, Memory, Disk, and Network Usage**.

**Step 2: Use Performance Monitor**

1. Open **Performance Monitor** (perfmon.msc).
2. Add counters like:
   * **Processor Time (%)**
   * **Disk Queue Length**
   * **Network Interface Usage**

**Step 3: Optimize Windows Services**

1. Open **services.msc**.
2. Disable unnecessary services:
3. net stop spooler
4. net stop wsearch
5. Disable background apps from **Task Manager** > **Startup**.

**Step 4: Disk Cleanup & Defragmentation**

1. Run cleanmgr to remove temporary files.
2. Run defrag C: to optimize disk performance.