**Module: 14-Identity with Windows Server**

**31. Installing and Configuring Hyper-V on Windows Server 2016**

**What is Hyper-V?**

Hyper-V is Microsoft’s built-in virtualization platform allowing multiple virtual machines (VMs) to run on a single physical server.

**Installation Steps:**

1. **Open Server Manager**
   * Click **Manage → Add Roles and Features**.
2. **Select Installation Type**
   * Choose **Role-based or feature-based installation**.
3. **Select Destination Server**
   * Choose the server you want to install Hyper-V on.
4. **Select Server Roles**
   * Check **Hyper-V**.
   * Click **Add Features** if prompted.
5. **Configure Virtual Switch**
   * During setup, you can create a virtual switch for VMs to connect to physical networks.
   * Choose network adapter to bind with the virtual switch.
6. **Confirm and Install**
   * Review selections and install.
   * Restart server if prompted.

**Post-Installation Configuration:**

* Open **Hyper-V Manager** (Tools → Hyper-V Manager).
* Create **Virtual Switches** (External, Internal, or Private).
* Create new virtual machines:
  + Define VM name, generation (Gen 1 or Gen 2).
  + Assign memory (static or dynamic).
  + Configure networking (attach to virtual switch).
  + Create or attach virtual hard disks.
* Install guest OS on VM.
* Configure checkpoints/snapshots for backup or rollback.

**Best Practices:**

* Use **Generation 2 VMs** when possible (secure boot, faster boot).
* Allocate **dynamic memory** cautiously.
* Separate **management OS network adapters** from VM traffic.
* Monitor resource usage (CPU, RAM, disk).

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

**Monitoring Performance:**

* **Task Manager**:
  + Quick view of CPU, memory, disk, and network utilization.
* **Performance Monitor**:
  + Open perfmon.
  + Add counters like % Processor Time, Available Memory, Disk Queue Length.
  + Use **Data Collector Sets** for logging performance over time.
* **Resource Monitor**:
  + Shows detailed usage per process.
* **Windows Admin Center**:
  + Centralized monitoring for multiple servers.
* **PowerShell**:
  + Use Get-Counter cmdlet for custom counters.

**Managing Event Logs:**

* Open **Event Viewer** .
* Categories:
  + **Application**: Application-level events.
  + **System**: OS component events.
  + **Security**: Auditing logins, policy changes.
* Create **Custom Views** to filter events.
* Configure **Event Subscriptions** to collect logs from multiple servers.
* Set **log size limits** and overwrite policies.
* Export logs for offline analysis.
* PowerShell:
  + Get-EventLog -LogName System -Newest 100
  + Get-WinEvent -LogName Security -MaxEvents 50

**33. Storage Options in Windows Server**

**1. Local Storage**

* Directly attached HDDs/SSDs.
* Use **Disk Management** or **Storage Spaces** to manage.

**2. Storage Spaces**

* Pool physical disks into virtual storage pools.
* Create resilient storage with **Mirroring** or **Parity**.
* Manage via Server Manager → File and Storage Services → Storage Pools.

**3. iSCSI**

* Block storage over IP.
* Configure iSCSI Targets (server side) and Initiators (client side).
* Useful for SAN-like storage without Fibre Channel hardware.

**4. Fibre Channel SAN**

* High-speed dedicated storage network.
* Requires HBAs and switches.

**5. SMB Shares**

* Network shares using Server Message Block protocol.
* SMB 3.0 supports encryption, multichannel for performance.

**6. Cluster Shared Volumes (CSV)**

* Enables multiple cluster nodes to access the same NTFS volume simultaneously.
* Used with Failover Clustering.

**7. ReFS (Resilient File System)**

* Designed for fault tolerance, large scale, data integrity.
* Used in Storage Spaces Direct and backup targets.

**8. Storage Replica**

* Synchronous/asynchronous block-level replication.
* Disaster recovery solution built-in to Windows Server.

**34. Role and Configuration of File Server**

**Role:**

* Central location for storing and sharing files.
* Provides access control, data availability, and versioning.

**Configuration:**

1. **Install File Server Role**
   * Server Manager → Add Roles → File and Storage Services → File Server.
2. **Create Shared Folders**
   * Right-click a folder → Properties → Sharing → Advanced Sharing.
   * Set share permissions.
3. **Set NTFS Permissions**
   * Control who can read/write/modify files.
4. **Enable Shadow Copies**
   * Right-click shared volume → Properties → Shadow Copies.
   * Allows users to restore previous file versions.
5. **Configure File Server Resource Manager (FSRM)**
   * Enforce quotas.
   * File screening to block certain file types.
   * Generate storage reports.
6. **Access-Based Enumeration**
   * Users only see files/folders they have permission to access.

**35. Implementing and Managing DFS**

**DFS Components:**

* **DFS Namespaces**: Virtual folder structure aggregating shared folders.
* **DFS Replication**: Syncs folders across servers.

**Steps:**

1. **Install DFS Roles**
   * Server Manager → Add Roles → DFS Namespaces and DFS Replication.
2. **Create Namespace**
   * DFS Management → Namespaces → New Namespace.
   * Choose domain-based (recommended).
   * Name it (e.g., \domain.local\shared).
3. **Add Folders to Namespace**
   * Add folder links pointing to shared folders on multiple servers.
4. **Configure DFS Replication**
   * New Replication Group → Add servers.
   * Define replication topology.
   * Select replicated folders.
   * Schedule replication time.
   * Monitor via DFS Management or PowerShell (Get-DfsrState).

**Best Practices:**

* Use domain-based namespaces.
* Plan replication topology carefully.
* Monitor replication health regularly.

**36. Built-in Backup and Recovery Options**

**Backup Tools:**

* **Windows Server Backup**:
  + File/folder, volume, system state, bare metal backups.
* **System State Backup**:
  + Critical OS components (registry, AD, boot files).
* **Shadow Copies (Previous Versions)**:
  + Enable on shared folders to let users recover files.
* **Active Directory Recycle Bin**:
  + Restore deleted AD objects.
* **Windows Recovery Environment (WinRE)**:
  + Bootable recovery tools including system restore, repair, bare-metal recovery.

**37. Configuring Windows Server Backup for Critical Data**

**Steps:**

1. Install Windows Server Backup feature.
2. Launch **Windows Server Backup**.
3. Select **Backup Schedule** → Create schedule.
4. Choose backup configuration:
   * Full server (all critical volumes).
   * Custom (select volumes/folders).
5. Choose backup destination:
   * External disk (recommended).
   * Network share.
6. Schedule backup frequency (daily/weekly).
7. Confirm settings and enable.
8. Optionally, enable email notifications via scripts or third-party tools.

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

1. Open **Windows Server Backup**.
2. Select **Recover**.
3. Choose backup location (local or remote).
4. Pick the backup date.
5. Choose **Files and Folders** recovery type.
6. Browse and select the files/folders to restore.
7. Select restore location:
   * Original location (overwrites existing).
   * Alternate location (safe for testing).
8. Complete recovery and verify files.

**39. Troubleshooting Windows Server Startup Issues**

**Common Problems:**

* Corrupted boot files.
* Driver conflicts.
* Hardware failures.
* Misconfigured boot loader.

**Techniques:**

* **Safe Mode Boot**: Press F8 during startup.
* **Startup Repair**: Boot from installation media → Repair.
* **Check Boot Configuration**: bcdedit /enum.
* **Run CHKDSK**: Fix disk errors.
* **SFC Scan**: sfc /scannow repairs system files.
* **Event Viewer**: Look for startup errors.
* **Disable recently added hardware/drivers**.
* **Last Known Good Configuration**.

**40. Troubleshooting Network Connectivity**

**Steps:**

* Verify IP config: ipconfig /all.
* Test connectivity: ping, tracert.
* Check DNS: nslookup.
* Check network adapter status.
* Use netsh to reset TCP/IP stack.
* Verify firewall rules.
* Use netstat to view open connections.
* Check cables and switch ports.
* Analyze packets with **Wireshark**.
* Restart network services: net stop/start.

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

**Issues:**

* Replication failures.
* Authentication errors.
* GPO not applying.
* DNS misconfiguration.
* Broken trusts.

**Troubleshooting:**

* Use **Dcdiag** for DC health.
* Use **Repadmin** to check replication.
* Verify DNS SRV records.
* Reset computer accounts with netdom reset.
* Check SYSVOL and NETLOGON shares.
* Verify trust relationships and reset if broken.
* Use **Event Viewer** for AD-specific logs.
* Use **Group Policy Results** (gpresult) for policy issues.

**42. Troubleshooting Performance Problems**

**Tools:**

* **Task Manager**, **Resource Monitor**.
* **Performance Monitor** with counters:
  + CPU (% Processor Time).
  + Memory (Available MB).
  + Disk (Avg. Disk Queue Length).
  + Network (Bytes/sec).

**Steps:**

* Identify high CPU/memory/disk usage.
* Check running processes causing load.
* Review recent changes (updates, apps).
* Check for memory leaks.
* Analyze paging file and virtual memory.
* Monitor network latency.
* Check for malware or resource-heavy services.
* Consider hardware upgrades if bottleneck persists