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

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

**Step 1: Install Hyper-V Role**

1. Open Server Manager: Start > Server Manager.
2. Add Roles and Features: Click on "Add Roles and Features" in the dashboard.
3. Role-Based Installation: Choose "Role-Based or Feature-Based Installation" and select your server.
4. Select Hyper-V: Check "Hyper-V" and click Next.
5. Configure Virtual Switches: Assign physical network adapters for virtual switches.
6. Confirm Installation: Review and click "Install." Restart the server if prompted.

**Step 2: Configure Hyper-V**

1. Open Hyper-V Manager: Access via Start menu > Administrative Tools > Hyper-V Manager.
2. Create Virtual Switches:
   * Open "Virtual Switch Manager" from the Actions pane.
   * Create external, internal, or private switches based on requirements.
3. Create Virtual Machines:
   * In Hyper-V Manager, click "New" > "Virtual Machine."
   * Follow the wizard to set up name, storage, memory, and network settings.
4. Adjust Settings: Configure VM resources (e.g., processors, disks, network) as needed.

**Step 3: Verify and Test**

1. Start a VM to ensure proper functionality.
2. Test network connectivity and resource allocation.

2] How do you monitor server performance and manage event logs in Windows

1. Performance Monitor:
   * Open "Performance Monitor" (Start > type perfmon).
   * Add counters (CPU, memory, disk, network) to monitor resource usage in real-time or log data for analysis.
2. Task Manager:
   * Access via Ctrl+Shift+Esc or right-click Taskbar > Task Manager.
   * Use the "Performance" tab for a quick view of resource usage.
3. Resource Monitor:
   * Launch from Task Manager > "Performance" tab > "Open Resource Monitor."
   * Monitor detailed resource utilization (CPU, Disk, Network).
4. Alerts:
   * Set up alerts in Performance Monitor to notify when thresholds are exceeded.

Managing Event Logs

1. Event Viewer:
   * Open "Event Viewer" (Start > type Event Viewer).
   * Navigate through categories (System, Application, Security) under "Windows Logs."
2. Filter Events:
   * Use "Filter Current Log" to find specific event types (e.g., errors, warnings).
3. Export/Archive Logs:
   * Right-click a log > "Save All Events As" to export logs for analysis.
4. Set Up Subscriptions:
   * Use Event Viewer > Subscriptions to collect logs from multiple servers**.**

**3] Describe the different types of storage options available in Windows Server.**

**Storage Options in Windows Server**

1. Direct-Attached Storage (DAS):
   * Locally attached to the server (e.g., internal hard drives or external USB drives).
   * Simple and cost-effective for single-server use.
2. Network-Attached Storage (NAS):
   * Shared storage accessible over a network.
   * File-based, suitable for centralized file sharing.
3. Storage Area Network (SAN):
   * High-performance, block-level storage connected via fiber channel or iSCSI.
   * Ideal for enterprise environments requiring scalability and redundancy.
4. Storage Spaces:
   * Software-defined storage feature in Windows Server.
   * Creates pools of physical disks for flexibility and redundancy.
5. Cluster Shared Volumes (CSV):
   * Used in failover clusters for shared storage access.
   * Optimized for Hyper-V and Scale-Out File Servers.
6. ReFS (Resilient File System):
   * Advanced file system for data integrity and large-scale storage.
   * Supports virtualization and high-availability workloads.
7. Cloud Storage Integration:
   * Connects to Azure Storage for hybrid storage solutions.
   * Extends local storage with cloud scalability.

**4] What is the role of File Server in Windows Server, and how do you configure it?**

The File Server role provides centralized file storage, sharing, and management. It allows users and applications to access files over a network securely and supports features like quotas, file screening, and DFS (Distributed File System).

**How to Configure File Server**

Step 1: Install File Server Role

1. Open Server Manager: Start > Server Manager.
2. Add Roles and Features: Select "File and Storage Services" > "File Server."
3. Confirm Installation: Review and install the role.

Step 2: Create and Share Folders

1. Create a Folder: Create a directory to share.
2. Share the Folder:
   * Right-click the folder > Properties > Sharing tab.
   * Click "Advanced Sharing," enable sharing, and assign permissions.
3. Set NTFS Permissions:
   * Use the "Security" tab to configure user or group access levels (Read, Write, Modify).

Step 3: Configure Additional Features (Optional)

1. Enable Quotas:
   * Use File Server Resource Manager (FSRM) to limit storage usage per user or folder.
2. Implement DFS:
   * Set up Distributed File System for centralized namespace and replication.
3. Enable File Screening:
   * Restrict certain file types using FSRM.

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

DFS allows centralized management and high availability of file shares across multiple servers.

**Step 1: Install DFS Roles**

1. **Open Server Manager:**  
   Start > Server Manager > "Add Roles and Features."
2. **Add DFS Namespaces and DFS Replication:**  
   Under "File and Storage Services," check **DFS Namespaces** and **DFS Replication** roles.
3. **Complete Installation:**  
   Click "Install" and restart if prompted.

**Step 2: Configure DFS Namespace**

1. **Open DFS Management:**  
   Start > Administrative Tools > DFS Management.
2. **Create Namespace:**
   * Right-click **Namespaces** > "New Namespace."
   * Select the host server and provide a namespace name (e.g., \\DomainName\Namespace).
   * Choose "Domain-based" or "Standalone" namespace type.
3. **Add Folder Targets:**
   * Right-click the namespace > "New Folder."
   * Add shared folders from different servers as targets.

**Step 3: Configure DFS Replication (Optional)**

1. **Create a Replication Group:**
   * In DFS Management, right-click "Replication" > "New Replication Group."
   * Choose "Multipurpose" or "Replication Group for DFS Namespace."
2. **Add Members and Folders:**
   * Specify servers and folders to replicate.
   * Configure replication topology (Hub-and-Spoke or Full Mesh).
3. **Set Bandwidth and Schedule:**
   * Define limits and timing for replication.

**Step 4: Manage and Monitor DFS**

1. **Access Namespace:**  
   Clients can access the namespace using \\DomainName\Namespace.
2. **Monitor Replication:**  
   Use **DFS Management** and **Event Viewer** to check replication status.
3. **Update Namespace:**  
   Add or remove folder targets as needed to adjust shared resources.

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

**Windows Server Backup (WSB):**

* Provides backup and recovery of files, folders, system state, and full server.
* Accessible via Server Manager > Add Features > "Windows Server Backup."
* Supports scheduling and storage on local drives or network shares.

**System State Backup:**

* Captures critical system components (Registry, AD, Boot Files).
* Useful for restoring Active Directory or system configurations.

**Bare Metal Recovery (BMR):**

* Enables recovery of the entire server onto similar hardware.
* Requires a full backup including system state.

**Volume Shadow Copy Service (VSS):**

* Creates snapshots of volumes for point-in-time recovery.
* Useful for recovering previous versions of files.

**File History and Previous Versions:**

* Allows users to restore individual files from earlier versions using shadow copies.

**Recovery Options:**

* Use Windows Recovery Environment (WinRE) for advanced troubleshooting.
* Boot from installation media for system repair.

**Cloud-based Backup (Optional):**

* Integrate with Azure Backup for secure, offsite data protection.

7] How do you configure Windows Server Backup to back up critical data?

1. **Install Windows Server Backup Feature**
   * Open **Server Manager** > "Add Roles and Features."
   * Navigate to "Features" and select **Windows Server Backup** > Install.
2. **Open Windows Server Backup**
   * Launch it from Start > Administrative Tools > **Windows Server Backup.**
3. **Configure Backup Schedule**
   1. **Click "Backup Schedule":** Choose a recurring backup schedule.
   2. **Select Backup Type:**
      * **Full Server Backup:** Covers the entire server.
      * **Custom Backup:** Select specific files, folders, or volumes.
   3. **Add Critical Data:**
      * Include system state, essential folders, and databases if needed.
4. **Choose Backup Destination**
   * **Local Drive:** Dedicated disk or volume.
   * **Network Share:** Enter the network path and credentials for shared storage.
   * **External Storage:** Use an external USB or NAS device.
5. **Set Schedule**
   * Specify the time and frequency of backups (e.g., daily, weekly).
   * Adjust according to business needs and data change rates.
6. **Confirm and Finish**
   * Review settings, confirm, and save the backup schedule.
7. **Test Backup and Recovery**
   * Run a manual backup to verify configuration.
   * Periodically test recovery to ensure data integrity.

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

1. **Safe Mode:**
   * Boot into Safe Mode by pressing **F8** or using installation media to access Advanced Boot Options.
   * Use it to identify and resolve driver or software conflicts.
2. **Last Known Good Configuration:**
   * Boot into **Advanced Options** and select this option to restore settings from the last successful login.
3. **Startup Repair:**
   * Boot from installation media and select **Repair your computer** > Troubleshoot > **Startup Repair**.
   * Automatically fixes missing or corrupted system files.
4. **Check Boot Order:**
   * Verify boot order in BIOS/UEFI to ensure the correct drive is prioritized.
5. **Run Command-Line Tools:**
   * **CHKDSK:** Fix disk errors: chkdsk /f /r.
   * **BOOTREC:** Repair boot records: bootrec /fixmbr, bootrec /fixboot, or bootrec /rebuildbcd.
6. **Disable Problematic Drivers/Services:**
   * Use **msconfig** or Safe Mode to disable recently added drivers or services.
7. **Event Viewer Analysis:**
   * Boot into recovery mode and check event logs for errors related to startup.
8. **Restore System State or Backup:**
   * Use Windows Server Backup to restore a known good configuration.
9. **Rebuild System Files:**
   * Run **SFC (System File Checker):** sfc /scannow to repair corrupted system files.
10. **Replace Hardware:**
    * Check for hardware failures like faulty RAM or hard drives that may prevent startup.

9] How do you troubleshoot network connectivity problems in Windows Server?

**Check Physical Connections:**

* Verify cables, network interfaces, and switches for proper connectivity.

**Verify IP Configuration:**

* Use ipconfig /all to check the server's IP address, subnet mask, default gateway, and DNS settings.
* Ensure static or DHCP-assigned IP is correct.

**Test Network Reachability:**

* Use **Ping:** Test connectivity to another device: ping <IP or Hostname>.
* **Tracert/Traceroute:** Trace the network path: tracert <IP or Hostname>.

**Check DNS Resolution:**

* Use nslookup <hostname> to verify DNS is resolving names correctly.
* Confirm DNS server settings.

**Examine Firewall Settings:**

* Check Windows Defender Firewall or third-party firewalls for blocked ports or rules.
* Use netsh advfirewall show allprofiles to view the current configuration.

**Inspect Network Adapter Settings:**

* Open **Network and Sharing Center** > "Change Adapter Settings."
* Ensure the adapter is enabled and configured correctly.

**Test with Alternate Network:**

* Use a different network or test from another device to isolate issues.

**Check for IP Conflicts:**

* Run arp -a to identify duplicate IP addresses on the network.

**Review Event Logs:**

* Open **Event Viewer** > "System Logs" to check for network-related errors.

**Use PowerShell Tools:**

* **Test-Connection:** To test ping-like connectivity.
* **Get-NetAdapter:** Review adapter status.
* **Get-NetIPConfiguration:** Display detailed IP settings.

**Restart Networking Services:**

* Use net stop "service name" and net start "service name" to restart services like DNS, DHCP Client, or NLA (Network Location Awareness).

**Update Drivers and Firmware:**

* Ensure network adapter drivers and firmware are up-to-date.

**Rebuild TCP/IP Stack:**

* Reset stack using netsh int ip reset and restart the server.

**Consult Logs and Diagnostics:**

* Use **Network Diagnostics Tool** in the Control Panel or PowerShell cmdlets for detailed analysis

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

**AD Replication Issues:**

* **Symptoms:** Changes not propagating across domain controllers.
* **Troubleshooting:**
  + Run repadmin /replsummary to check replication health.
  + Use dcdiag to diagnose domain controller issues.
  + Verify DNS configuration and connectivity between domain controllers.

**Authentication Failures:**

* **Symptoms:** Users unable to log in or access resources.
* **Troubleshooting:**
  + Check user account status (locked, disabled, expired).
  + Ensure correct time synchronization (use w32tm to sync).
  + Verify Kerberos tickets using klist.

**DNS Configuration Problems:**

* **Symptoms:** AD services depend on DNS; incorrect DNS causes login and resource access failures.
* **Troubleshooting:**
  + Verify DNS settings with nslookup.
  + Check SRV records in DNS Manager.
  + Restart DNS service if needed.

**Group Policy Issues:**

* **Symptoms:** Policies not applied or inconsistent behavior.
* **Troubleshooting:**
  + Use gpresult /h and rsop.msc to analyze Group Policy application.
  + Verify GPO links, permissions, and replication.

**FSMO Role Failures:**

* **Symptoms:** AD functions like password resets or schema updates fail.
* **Troubleshooting:**
  + Identify FSMO role holders with netdom query fsmo.
  + Transfer or seize FSMO roles using NTDSUTIL if necessary.

**Account Lockouts:**

* **Symptoms:** Frequent account lockouts for users.
* **Troubleshooting:**
  + Use Event Viewer to track logon attempts (Event ID 4740).
  + Check mapped drives or services using stale credentials.

**AD Database Corruption:**

* **Symptoms:** Inconsistent behavior or directory service errors.
* **Troubleshooting:**
  + Run NTDSUTIL to perform database integrity checks.
  + Restore from backup if corruption is severe.

**Domain Controller Down:**

* **Symptoms:** Unable to authenticate or manage AD.
* **Troubleshooting:**
  + Check server status and network connectivity.
  + Use dcdiag and Event Viewer to diagnose.
  + Restore domain controller from a backup if needed.

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

**Troubleshooting Performance Problems on Windows Server 2016/2019**

1. **Check Resource Usage with Task Manager/Resource Monitor:**
   * **Task Manager:** Monitor CPU, memory, disk, and network usage (Ctrl+Shift+Esc).
   * **Resource Monitor:** Provides more detailed insights into resource usage.
2. **Use Performance Monitor:**
   * Open **PerfMon** and add performance counters (CPU, memory, disk, network) for real-time data collection.
   * Set alerts for high resource usage.
3. **Check Event Logs:**
   * Open **Event Viewer** and check for warnings and errors related to system performance under **System** and **Application** logs.
4. **Analyze Disk Performance:**
   * Use **Task Manager** > "Performance" tab to monitor disk I/O.
   * Run chkdsk to check for disk errors.
   * Ensure there’s enough free space on system and data drives.
5. **Monitor Network Performance:**
   * Check network adapter settings, cables, and configurations.
   * Use **ping** or **tracert** to check network latency or packet loss.
6. **Check for Software Issues:**
   * Check for high resource usage by processes in **Task Manager**.
   * Update drivers or uninstall problematic software.
7. **Run System Diagnostics:**
   * Use **System Configuration (msconfig)** to disable unnecessary startup services and apps.
   * Check for unnecessary background processes.
8. **Verify System Configuration:**
   * Ensure system settings (e.g., Virtual Memory/Page File) are optimized.
   * Run **sfc /scannow** to check and repair system files.
9. **Check for Malware or Security Threats:**
   * Run a full antivirus scan or use Windows Defender to check for malware impacting performance.
10. **Update Drivers and Firmware:**

* Ensure that hardware drivers and firmware are up-to-date for optimal system performance.