Module: 14- Identity with Windows Server

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

Ans –

❖ Installing the Hyper-V Role:

- Using Server Manager:

    1. Open Server Manager.
    2. Click "Manage" and then "Add Roles and Features."
    3. Follow the wizard, selecting "Role-based or feature-based installation."
    4. Select the server where you want to install Hyper-V.
    5. On the "Select server roles" page, check the "Hyper-V" box.
    6. In the pop-up window, click "Add Features."
    7. Continue through the wizard, configuring any necessary options, and then click "Install."
    8. The server may need to restart.

❖ Configuring Hyper-V:

- Virtual Switch Manager:

    1. Open Hyper-V Manager.
    2. In the Actions pane, click "Virtual Switch Manager."
    3. Choose the type of virtual switch you want to create:
        i. External: Connects virtual machines to the physical network.
        ii. Internal: Connects virtual machines to each other and to the host computer.
        iii. Private: Connects virtual machines to each other only.
    4. Select the appropriate network adapter and click "Create Virtual Switch."
    5. Configure the virtual switch settings, such as VLANs, and click "OK."

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

Ans –

1. Monitoring Server Performance:

- Task Manager:

    - Provides a quick overview of real-time CPU, memory, disk, and network usage.

    - Useful for identifying processes that are consuming excessive resources.

- Resource Monitor:

    - Offers more detailed real-time information about resource utilization.
    - Provides insights into which processes are using specific resources.
    - Helps in identifying bottlenecks.

- Performance Monitor:

    - A powerful tool for collecting and analyzing performance data over time.
    - Allows you to create data collector sets to track specific performance counters.
    - Enables you to identify trends and potential performance issues.

2. Managing Event Logs:

- Event Viewer :
    - The primary tool for viewing and managing event logs.
    - Provides access to various event logs, including Application, Security, and System logs.
    - Allows you to filter and search for specific events.
    - Enables you to create custom views to focus on specific event types.

Key Event Logs:

- Application Log:
    - Records events from applications and programs.
- Security Log:
    - Records security-related events, such as logon attempts and access control changes.
- System Log:
    - Records events from Windows system components, such as drivers and services.

Event Log Management Best Practices:

- Regularly Review Event Logs:
    - Check for errors and warnings that may indicate potential problems.
- Filter and Search Event Logs:
    - Use filters to focus on specific event types or time ranges

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

Ans - 1. Direct-Attached Storage (DAS):

- This involves storage devices directly connected to the server, such as hard disk drives (HDDs) or solid-state drives (SSDs).
- This is the most basic form of storage and is suitable for applications that require high performance and low latency.
- Examples:
  - Internal SATA or SAS drives.
  - External drives connected via USB or Thunderbolt.

2. Network-Attached Storage (NAS):

- NAS devices are dedicated file servers that connect to the network, providing file-level access to multiple clients.
- They are ideal for file sharing, backups, and archiving.
- NAS devices typically use protocols like Server Message Block for Windows environments and NFS (Network File System) for Linux.

3. Storage Spaces:

- This is a software-defined storage solution built into Windows Server that allows you to pool multiple physical drives into virtual storage spaces.
- It provides features like:
  - Storage resiliency (e.g., mirroring, parity) to protect against drive failures.
  - Storage tiering to optimize performance by moving frequently accessed data to faster drives.
- Storage spaces direct (S2D): which allows for the creation of software defined storage using local storage on clustered servers.

4. Cloud Storage:

- Windows Server can integrate with cloud storage services, such as Azure Storage, to provide off-site backups, archiving, and disaster recovery.
- Cloud storage offers scalability, flexibility, and cost-effectiveness.

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

Ans - Role of a File Server:

- Centralized File Storage:
  - A File Server acts as a central repository for files, allowing multiple users to store and access data in a shared location.
- File Sharing and Access Control:
  - It enables controlled sharing of files and folders with specific users or groups, using NTFS permissions and share permissions.
- Data Management:
  - It facilitates efficient data management, including organizing, backing up, and restoring files.
- Enhanced Collaboration:
  - It promotes collaboration by allowing multiple users to work on shared files simultaneously.
- Data Security:
  - It provides security features to protect sensitive data through access control and encryption.

Configuration:

Here's a general overview of how to configure a File Server in Windows Server:

1. Installing the File Server Role:
   - Use Server Manager to add the "File and Storage Services" role, specifically the "File Server" role service.
   - Alternatively, you can use PowerShell commands to install the role.
2. Creating Shared Folders:
   - Create folders on the server's storage drives that you want to share.
   - Right-click on the folder and select "Properties."
   - Go to the "Sharing" tab and click "Advanced Sharing."
   - Enable "Share this folder" and configure the share name and permissions.
3. Configuring Permissions:
   - Share Permissions:
     - Control access to the shared folder over the network.
     - Allow or deny access to users and groups.
   - NTFS Permissions:
     - Control access to files and folders within the shared folder.
     - Provide granular control over read, write, modify, and other permissions.

   - It is very important to understand the difference between share permissions, and NTFS permissions, and how they interact with each other.
4. Implementing Security Best Practices:

   - Use strong passwords and access control lists (ACLs).
   - Regularly update the server with security patches.
   - Implement data encryption and backups.
   - Consider using Access-based enumeration, so users only see the files and folders that they have permissions to access.
5. Utilizing DFS (Distributed File System):
   - DFS Namespaces: Create a logical view of shared folders across multiple servers.

   - DFS Replication: Replicate files between servers for redundancy and availability.
6. Storage Management:
   - Ensure adequate storage capacity and performance.
   - Consider using RAID configurations for data redundancy.
   - Implement data deduplication to reduce storage consumption.

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

Ans - 1. Understanding DFS:

- DFS Namespaces:
  - Creates a logical, hierarchical view of shared folders located on different servers.
  - Provides a single, unified namespace for users to access files, regardless of their physical location.
  - Improves file availability and simplifies file access.
- DFS Replication:
  - Replicates files and folders between multiple servers.
  - Ensures data redundancy and availability in case of server failures.
  - Helps distribute file access load across multiple servers.

2. Installing DFS Roles:

- Open Server Manager.
- Click "Manage" and then "Add Roles and Features."
- Select "Role-based or feature-based installation."
- Select the server where you want to install DFS.
- On the "Select server roles" page, expand "File and Storage Services" and then "File and iSCSI Services."
- Check the boxes for "DFS Namespaces" and "DFS Replication."
- Complete the wizard and install the roles.

3. Configuring DFS Namespaces:

- Create a Namespace:
  - Open DFS Management (dfsmgmt.msc).
  - Right-click "Namespaces" and select "New Namespace."
  - Enter the server name that will host the namespace.
  - Choose a namespace type:
    - Domain-based namespace: Stores namespace information in Active Directory, providing high availability.
    - Standalone namespace: Stores namespace information on a single server.
  - Enter a namespace name (e.g., \\yourdomain\Files).
  - Configure namespace settings, such as access-based enumeration.
  - Click "Create."
- Add Namespace Folders:
  - In DFS Management, navigate to your namespace.
  - Right-click the namespace and select "New Folder."
  - Enter a folder name
  - Add Folder Targets:
    - Click the add button, and add the network path to the actual shared folders that you want to be accessed when a user accesses the namespace folder.
    - This links the logical namespace folder to the physical shared folders on your servers.
- Configure Folder Targets:
  - You can configure settings for folder targets, such as priority and referral ordering.

4. Configuring DFS Replication:

- Create a Replication Group:
  - In DFS Management, right-click "Replication" and select "New Replication Group."
  - Choose a replication group type (e.g., "Multipurpose replication group").
  - Enter a replication group name.
  - Add the servers that will participate in replication.
  - Choose the replication topology (e.g., "Full mesh").
  - Select the folders to replicate.
  - Configure bandwidth and scheduling settings.
  - Review and create the replication group.
- Configure Replication Settings:
  - You can configure settings such as staging folder size, conflict resolution, and replication scheduling.
- Initial Replication:
  - DFS Replication will perform an initial replication of the files and folders.

  - It is best practice to pre-seed large amounts of data to speed up this process.

5. Managing DFS:

- Monitor DFS Health:
  - Use DFS Management to monitor the health of namespaces and replication groups.
  - Check for errors and warnings.

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

Ans - 1. Windows Server Backup (WSB):

- Role-Based Backup:
  - WSB allows you to back up entire servers, specific volumes, system state, or individual files and folders.
- Scheduled Backups:
  - You can schedule backups to run automatically at specific intervals.
- Backup Destinations:
  - WSB supports backing up to local drives, network shares, or dedicated backup drives.
- Bare Metal Recovery:
  - WSB enables bare metal recovery, which allows you to restore an entire server to a different hardware configuration.
- System State Backup:
  - This critical feature captures the operating system files, Active Directory, and other system-level configurations.

2. Recovery Options:

- File and Folder Recovery:
  - WSB allows you to restore individual files and folders from a backup.
- Volume Recovery:
  - You can restore entire volumes from a backup.
- System State Recovery:
  - You can restore the system state to recover operating system configurations.
- Bare Metal Recovery:
  - This allows you to restore an entire server to a new or different hardware configuration.

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

Ans - 1. Install Windows Server Backup:

- Using Server Manager:
  - Open Server Manager.
  - Click "Manage" > "Add Roles and Features."
  - Follow the wizard, selecting "Features."
  - Check the "Windows Server Backup" box.
  - Complete the installation.
- This installs the necessary tools for backup and recovery.

2. Backup Strategy:

- Identify Critical Data:
  - Determine which files, folders, and applications are essential for your business operations. This includes databases, application data, and user files.
- Choose Backup Type:
  - Full Server: Backs up everything, including the operating system, applications, and data. Ideal for disaster recovery.
  - Custom: Allows you to select specific volumes, folders, or files. Useful for backing up critical data only.
  - System State: Backs up the operating system files, Active Directory, and other system configurations. Essential for recovering from system failures.
- Set Backup Frequency:
  - Determine how often backups should occur based on the rate of data change and your recovery point objective.
- Choose Backup Destination:
  - Dedicated Backup Drive: Recommended for optimal performance and reliability.
  - Network Share: Suitable for smaller backups or when a dedicated drive is not available.
  - Important: Avoid backing up to the same drive as your critical data.

3. Configure Windows Server Backup:

- Open Windows Server Backup:
  - Search for "Windows Server Backup" in the Start menu.
- Configure a Scheduled Backup:
  - In the Actions pane, click "Backup Schedule."
  - Follow the wizard:
    - Choose the backup configuration (Full Server or Custom).
    - If choosing custom, carefully select the volumes or folders containing your critical data.
    - Set the backup time and frequency.

        - Select the backup destination.
        - Review and confirm the settings.

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

Ans - 1. Open Windows Server Backup:

- Search for "Windows Server Backup" in the Start menu and open it.

2. Initiate the Recovery Wizard:

- In the Actions pane, click "Recover."
- This will launch the Recovery Wizard.

3. Select the Backup Location:

- Choose where the backup is stored:
    - "This server" (if the backup is on a local drive).
    - "A backup stored on another location" (if the backup is on a network share or another drive).
- Click "Next."

4. Specify Location Type:

- If you selected "A backup stored on another location," you'll need to specify the location type (e.g., "Remote shared folder").
- Input the network path to the backup location, and if needed, credentials to access that network share.
- Click "Next".

5. Select the Backup Date and Time:

- Choose the specific backup version (date and time) that contains the files and folders you want to restore.
- Click "Next."

6. Select Recovery Type:

- Choose "Files and folders."
- Click "Next."

7. Select Items to Recover:

- Browse through the backup contents and select the specific files and folders you want to restore.
- You can expand folders to select individual files.
- Click "Next."

8. Specify Recovery Options:

- Choose where to restore the files and folders:
    - "Original location": Restores the files to their original location.
    - "Alternate location": Restores the files to a different folder. You'll need to specify the alternate location.
- Choose what to do if existing files with the same name are found:
    - "Create copies so that you have both versions."
    - "Overwrite the existing versions."
    - "Do not recover the selected items."
- Click "Next."

9. Confirm and Start Recovery:

- Review the recovery settings.
- Click "Recover" to begin the restore process.

10. Completion:

- Wait for the recovery process to complete.
- Once finished, you can verify that the files and folders have been restored successfully.

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

Ans - 1. Initial Checks:

- Hardware Inspection:
    - Ensure all power cables and connections are secure.
    - Check for any recent hardware changes that might be causing conflicts.
    - Listen for any unusual sounds from the hard drives or other components.
- BIOS/UEFI Checks:
    - Verify that the boot order is correct.
    - Check for any hardware errors reported in the BIOS/UEFI.
    - Ensure that virtualization settings (if used) are correctly configured.

2. Windows Recovery Environment (Windows RE):

- Accessing Windows RE:
  - If the server fails to start, Windows RE should automatically launch.
  - You can also access it by booting from a Windows Server installation disc or USB drive and selecting "Repair your computer."
- Startup Repair:
  - This automated tool can fix many common startup problems, such as corrupted boot files.
- System Restore:
  - Rolls back the system to a previous restore point, which can be helpful if recent software changes caused the problem.
- Safe Mode:
  - Starts Windows with a minimal set of drivers and services, which can help isolate software conflicts.

3. Boot-Related Issues:

- Boot Configuration Data (BCD) Errors:
  - Use the bootrec command-line tools to repair BCD errors.
- Corrupted Boot Files:
  - Use the sfc /scannow command to repair corrupted system files.
- Master Boot Record (MBR) Issues:
  - Use the bootrec /fixmbr command to repair MBR issues.

4. Driver Issues:

- Safe Mode:
  - Boot into Safe Mode to disable or uninstall recently installed drivers.
- Device Manager:
  - Use Device Manager in Windows RE or Safe Mode to check for driver errors.

5. Event Logs:

- Event Viewer:
  - Access Event Viewer in Windows RE or after the server starts to check for error messages that can provide clues about the cause of the startup problem.

6. Hardware Troubleshooting:

- Memory Tests:
  - Use a memory testing tool to check for memory errors.
- Hard Drive Tests:
  - Use a hard drive diagnostic tool to check for hard drive errors.

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

Ans - 1. Physical Layer Checks:

- Cable Connections:
  - Ensure all network cables are securely connected to the server and network devices (switches, routers, modems).
  - Check for damaged or frayed cables.
- Network Adapter Status:
  - Verify that the network adapter is enabled in Device Manager.
  - Check the network adapter's link lights for activity.
  - If possible, try a different network cable or port.
- Switch/Router Status:
  - Confirm that network switches and routers are powered on and functioning correctly.

2. DNS Troubleshooting:

- nslookup:
  - Use the nslookup command to check DNS resolution.
  - This tool can help determine if DNS servers are resolving hostnames correctly.
- Flush DNS Cache:
  - Use the ipconfig /flushdns command to clear the DNS cache.

3. Firewall Checks:

- Windows Firewall:
  - Verify that Windows Firewall is not blocking necessary network traffic.
  - Check firewall rules to ensure that required ports are open.
  - Temporarily disabling the firewall can help determine if the firewall is the cause of the problem.
- Third-Party Firewalls:
  - If you are using a third-party firewall, check its configuration.

4. Network Services:

- Network and Sharing Center:
  - Use the Network and Sharing Center to check network connections and settings.

- Services:
  - Verify that network-related services, such as DHCP Client and DNS Client, are running.

5. Event Logs:

- Event Viewer:
    - Check the Event Viewer for network-related errors and warnings.

6. Advanced Troubleshooting:

- Network Monitor/Wireshark:
    - Use network monitoring tools like Wireshark to capture and analyze network traffic. This can help identify network protocol issues.
- netstat:
    - The netstat command is useful for displaying network connections, routing tables, and network interface statistics.

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

Ans - 1. Replication Failures:

- Symptoms:
    - Inconsistent data across domain controllers (DCs).
    - Login problems.
    - Group Policy application failures.
- Troubleshooting:
    - repadmin /replsummary: Checks replication status.
    - repadmin /showrepl: Displays detailed replication information.
    - dcdiag /v: Performs comprehensive DC diagnostics.
    - Event Viewer: Check the Directory Service event log for replication errors.
    - Firewall Issues: Ensure that the necessary ports for AD replication are open (e.g., TCP 135, 389, 445, and dynamic ports).
    - DNS Issues: Verify that DNS is configured correctly, and DCs can resolve each other's names.
    - Time Synchronization: Ensure that all DCs have accurate time synchronization.

2. DNS Issues:

- Symptoms:
    - Login failures.
    - Name resolution problems.
    - Replication failures.
- Troubleshooting:
    - nslookup: Checks DNS resolution.
    - dcdiag /test:dns: Performs DNS-related tests.

    - Verify that the DNS server is configured to allow dynamic updates.
    - Ensure that the AD-integrated DNS zones are correctly configured.
    - Verify that the DNS records for the DCs are correct.

3. Group Policy Issues:

- Symptoms:
    - Group Policy settings not being applied.
    - Application errors.
- Troubleshooting:
    - gpresult /r: Displays applied Group Policy settings.
    - gpupdate /force: Forces a Group Policy update.
    - Event Viewer: Check the Application and System event logs for Group Policy errors.
    - rsop.msc (Resultant Set of Policy): Provides a detailed view of applied Group Policy settings.
    - Verify that the Group Policy objects (GPOs) are linked correctly.
    - Check for file replication service(FRS) or DFSR issues if the GPO's are not replicating.

4. Login Issues:

- Symptoms:
    - Users unable to log in.
    - "Incorrect username or password" errors.
- Troubleshooting:
    - Verify that the user account is enabled.
    - Check for account lockout policies.
    - Ensure that the user is logging in to the correct domain.
    - Verify that the DC is available and responding.
    - Check for time synchronization issues.
    - Check for DNS issues.

5. Account Lockouts:

- Symptoms:
    - Users being locked out of their accounts.
- Troubleshooting:
    - Event Viewer: Check the Security event log for account lockout events.
    - Use the Account Lockout Status tool (account lockout tools) to identify the DC where the lockout occurred.
    - Identify the source of the bad password attempts.
    - Check for cached credentials, mapped drives, or scheduled tasks that might be using old passwords.

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

Ans - 1. Establish a Baseline:

- Before troubleshooting, establish a baseline of normal server performance. This involves monitoring key performance counters during typical server operation. This helps you identify deviations from normal behavior.

2. Identify the Symptoms:

- Slow application performance.
- High CPU utilization.
- High memory utilization.
- High disk I/O.
- Network latency.
- Application crashes or freezes.

3. Use Performance Monitoring Tools:

- Task Manager:
  - Provides a quick overview of CPU, memory, disk, and network utilization.
  - Useful for identifying processes consuming excessive resources.
- Resource Monitor (resmon.exe):
  - Offers more detailed real-time information about resource usage.
  - Provides insights into which processes are using specific resources.
  - Helps identify resource contention.
- Performance Monitor (perfmon.msc):
  - A powerful tool for collecting and analyzing performance data over time.
  - Allows you to create data collector sets to track specific performance counters.
  - Essential for identifying trends and bottlenecks.
- Event Viewer (eventvwr.msc):
  - Examine application, system, and security logs for errors or warnings that may indicate performance issues.