Windows Server Security And Maintenance

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

In my practical setup, I installed and configured Hyper-V on Windows Server 2022 Database Edition, which I was running inside VMware on a Windows 10 host system. The process is similar to

Windows Server 2016, so the steps apply equally. First, I opened Server Manager from the Start Menu. Then, I clicked on Add Roles and Features, which started the installation wizard. I selected Role-based or feature-based installation, then selected my local server from the list. After that, I checked the Hyper-V role and allowed the wizard to include all required features automatically. Next, the wizard asked about Virtual Switches — I selected my network adapter to allow virtual machines to access the external network. After confirming the selections, I clicked Install and allowed the system to restart when required. Once the installation completed, I opened Hyper-V Manager from the Administrative Tools section. Inside Hyper-V Manager, I created a Virtual Switch using the Virtual Switch Manager, and then I created a new Virtual Machine (VM) by specifying the VM name, generation (Gen 1 or Gen 2), memory size, network adapter, and virtual hard disk size. After configuring these options, I attached an ISO file to the VM to install the guest operating system. Finally, I powered on the VM and completed the OS installation inside Hyper-V. Through this, I successfully used Hyper-V to create and manage virtual machines on my Windows Server. Hyper-V provided excellent resource management and isolation features that were especially useful in a virtual lab environment like mine.

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

Monitoring server performance and managing event logs are essential tasks in any Windows Server environment to ensure system stability and detect problems early. On my Windows Server 2022 running in VMware, I used two main tools: Performance Monitor and Event Viewer. To monitor performance, I opened Performance Monitor from the Start Menu. This tool allowed me to track key performance counters like CPU usage, available memory, disk I/O, and network utilization. I added specific counters for “Processor Time (%)” and “Memory Pages/sec” to monitor system load. Performance Monitor also allows creating Data Collector Sets, which can record data over time for trend analysis. I set up one to monitor CPU and RAM usage every 30 seconds to analyze how my VMs affected the server performance. For managing logs, I opened Event Viewer, which records all important system and security events. Inside it, I explored different sections like Application, System, and Security logs. I filtered warnings and errors to detect potential issues such as failed logons, service crashes, or driver errors. When I noticed repetitive network warnings, I used the log details to identify misconfigurations in the VMware network adapter. Regular monitoring using these tools helps ensure that the server performs smoothly and any issues are detected and resolved quickly.

33. Describe the different types of storage options available in Windows Server. Windows Server offers several storage options suitable for different organizational needs and environments. During my practical work on Windows Server 2022 in VMware, I explored various storage types such as Direct-Attached Storage (DAS), Network-Attached Storage (NAS), and Storage Area Network (SAN). Direct-Attached Storage (DAS) refers to storage directly connected to the server through physical interfaces like SATA or NVMe drives. It is simple and cost-effective, ideal for standalone servers or testing environments like mine. Network-Attached Storage (NAS) connects to the network using standard Ethernet and shares files through protocols such as SMB (Server Message Block). It allows multiple systems to access the same storage simultaneously, making it suitable for file sharing in small networks. Storage Area Network (SAN) is a high-performance option that connects servers and storage devices over a dedicated network using technologies like iSCSI or Fibre Channel. It’s used in enterprise environments where speed and redundancy are critical. Windows Server also supports Storage Spaces, which lets administrators group multiple drives into a single pool and create virtual disks with redundancy options like mirroring or parity. I also learned about ReFS (Resilient File System), which protects data integrity and supports automatic error correction. Lastly, Cluster Shared Volumes (CSV) allow multiple servers in a failover cluster to access the same volume, providing high availability.

34. What is the role of File Server in Windows Server, and how do you configure it?
The File Server role in Windows Server is used to centrally store and manage files so that users and applications on a network can access them securely and efficiently. In my setup on Windows Server 2022 running in VMware, I installed and configured the File Server role to understand its functionality. To begin, I opened Server Manager and selected Add Roles and Features. I chose Role-based or feature-based installation, selected my local server, and under File and Storage Services, I checked the File Server role. Once installation finished, I used File and Storage Services in Server Manager to create shared folders. I right-clicked on Shares, selected New Share, and chose the SMB Share - Quick option. I specified the folder path and gave it a shared name like “StudentData.” Then, I configured permissions by allowing specific users (for example, administrators or certain user groups) access with either Read or Full Control. After finishing the wizard, the shared folder became accessible from other systems on my VMware network using the path \\servername\StudentData. The File Server also supports advanced features like File Server Resource Manager (FSRM), which helps monitor storage usage and set quotas, and Shadow Copies, which enable restoring previous versions of files. By using these tools, I learned how Windows Server can efficiently handle file sharing, security, and backup for multiple users in an enterprise environment.

35. Explain the process of implementing and managing Distributed File System (DFS) in Windows Server 2016.
Distributed File System (DFS) is a Windows Server feature that allows multiple shared folders on different servers to appear as a single logical namespace. This makes file access easier for users and provides redundancy for fault tolerance. In my practical environment using Windows Server 2022 on VMware, I implemented DFS Namespaces and DFS Replication to understand how it works. First, I opened Server Manager → Add Roles and Features. In the wizard, I selected Role-based or feature-based installation, chose my server, and under File and Storage Services, I enabled both DFS Namespaces and DFS Replication. Once the installation completed, I went to Tools → DFS Management from the Server Manager menu. In the DFS Management console, I right-clicked Namespaces and selected New Namespace. I chose my local server as the host, then entered a namespace name like “CampusData.” After setting permissions, the namespace was created. Inside the namespace, I added folder targets — shared folders located on different servers or drives, such as “C:\StudentData” and “D:\ProjectData.” This allowed both folders to be accessed from a single path, such as \\ServerName\CampusData. To provide fault tolerance, I configured DFS Replication. I created a new replication group and added both shared folders as targets. Then, I selected Full Mesh topology to allow both servers to replicate changes to each other. Finally, I set replication schedules and bandwidth usage. Once replication began, any file created or modified in one folder automatically synchronized to the other. DFS makes file access simple and ensures high availability, which is very useful in large networks or multi-branch organizations.

36. Discuss the built-in backup and recovery options available in Windows Server 2016 or 2019. Windows Server provides several built-in tools for data backup and disaster recovery, helping administrators protect critical information from loss or corruption. While doing practical work on
Windows Server 2022 inside VMware, I used Windows Server Backup (WSB), Volume Shadow Copy Service (VSS), and System Restore. Windows Server Backup allows full server, system state, or custom folder backups. It can be scheduled or run manually and supports local disks, external drives, and network shares. This is ideal for recovering from hardware failures or accidental data loss. Volume Shadow Copy Service (VSS) enables snapshots of volumes while the system is running, so files can be restored to earlier versions even when applications are open. This helps users recover old versions of files without performing a full backup restore. System

Restore focuses on configuration-level recovery. It allows rolling back system files and registry settings to a previous state, useful after a failed update or misconfiguration. Additionally, Windows Recovery Environment
(WinRE) provides tools such as Startup Repair and Command Prompt for advanced troubleshooting. Together, these options give administrators flexibility to recover files, applications, or the full server environment depending on the severity of the issue.

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

To configure Windows Server Backup (WSB) for protecting critical data on my Windows Server 2022 virtual machine, I first ensured that the feature was installed. I opened Server Manager → Add Roles and Features, then under Features, I selected Windows Server Backup. After installation, I opened the Windows Server Backup console from Administrative Tools. I chose Backup Schedule to automate backups. The wizard prompted me to select what to back up — I selected Custom, then added the folders containing student and project data. Next, I specified the backup destination. Since I was using VMware, I attached an external virtual hard disk (VHD) and selected it as the backup location. This kept backups separate from the system drive. I configured the schedule to run daily at midnight to ensure consistent protection. For one-time backups, the Backup Once option can be used instead. The wizard allowed me to enable VSS full backup, which clears backup logs and maintains consistency. After confirming settings, WSB began the backup and displayed progress in real time. Once finished, I verified the backup file on the destination drive. The configuration ensured that my system could recover essential data even if the primary storage became corrupted or lost.

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

Restoring files and folders using Windows Server Backup is straightforward. On my Windows Server 2022 system, I opened the Windows Server Backup console and selected the Recover option from the right-hand panel. The wizard asked me to choose where the backup was stored — I selected This server since my backup was on a local virtual disk. Next, I chose the backup date from the calendar. Under Recovery Type, I selected Files and Folders, then browsed through the backup contents to locate the folder I wanted to restore. The wizard offered two options: Original location or Alternate location. To avoid overwriting files, I selected an alternate path (like “D:\RestoredData”). Before proceeding, I reviewed the summary and clicked Recover. The restore process began and showed progress for each file. Once completed, I verified the recovered data. Windows Server Backup also preserves NTFS permissions, so user access settings remain intact. If a system drive or OS corruption occurs, a System State Restore or Bare Metal Recovery can also be performed. This ensures full system recovery, which is especially useful for domain controllers or servers handling critical roles.

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

When a Windows Server fails to start properly, several techniques can be used to diagnose and fix the issue. In my VMware-based Windows Server 2022 environment, I simulated startup errors and learned to troubleshoot them using built-in tools. First, I booted into the Advanced Startup Options by pressing F8 or through the recovery menu. From there, I selected Safe Mode, which loads only essential drivers and services. If the system started successfully in Safe Mode, the problem was likely caused by a faulty driver or recently installed software. Next, I tried Last Known Good Configuration, which restores the system to the last successful boot setup. When system files were corrupted, I used Startup Repair in the Windows Recovery Environment (WinRE). This tool automatically detects and repairs missing or damaged boot files. If that failed, I accessed Command Prompt from recovery tools and ran commands like bootrec /fixmbr, bootrec /fixboot, and sfc /scannow to repair the boot loader and check system integrity. In case of hardware issues, I checked virtual disk connections in VMware and BIOS boot order. Using these methods, I learned how to diagnose whether the issue was software-based or hardware-related and perform targeted recovery steps effectively.

40. How do you troubleshoot network connectivity problems in Windows Server?
Troubleshooting network issues in Windows Server involves a systematic approach. In my Windows Server 2022 setup on VMware, I faced network connectivity issues when my virtual machine couldn’t access the internet. To fix this, I started by checking the Network Adapter settings in Control Panel → Network and Sharing Center → Change Adapter Settings. I ensured that the adapter was enabled and connected to the correct VMware network (usually “Bridged” or “NAT”). Next, I opened Command Prompt and ran ipconfig /all to check the IP configuration. If the IP address was missing or incorrect, I used ipconfig /release and ipconfig /renew to refresh it. Then, I pinged the gateway and other systems using ping to test connectivity. If DNS resolution failed, I ran nslookup to verify the DNS server configuration. I also checked Windows Firewall to ensure it wasn’t blocking connections. If needed, I temporarily disabled it for testing. Additionally, Event Viewer logs under “System” helped me identify DHCP or DNS-related errors. Sometimes the issue was on the VMware side, such as when the virtual network adapter wasn’t properly connected. Reconfiguring the VMware network settings usually resolved the problem. By following these steps, I was able to consistently restore network connectivity on my server.

41. Discuss common Active Directory-related issues and their troubleshooting steps.
Active Directory (AD) issues can disrupt authentication, replication, and access control across the network. While working on Windows Server 2022, I encountered and studied several AD-related problems and how to resolve them. One common issue is replication failure between domain controllers. I used the repadmin /replsummary and repadmin /showrepl commands to check replication health. If replication was failing, I verified DNS settings since AD heavily relies on DNS. Misconfigured DNS zones or missing SRV records are frequent causes. Another issue involves user authentication failures, often due to time differences between domain controllers and clients. I synchronized time using the w32tm /resync command. For account lockouts, I used Active Directory Users and Computers (ADUC) to reset passwords or unlock accounts. Group Policy errors are also common. To troubleshoot, I ran gpresult /h report.html to generate a detailed policy report and reviewed Event Viewer → Group Policy Operational Log. If Group Policy Objects (GPOs) were not updating, I used gpupdate /force to refresh them. In some cases, restoring System State Backup helped recover AD databases after corruption. These troubleshooting methods helped me understand how to maintain a stable and healthy Active Directory environment.

42. Explain how to troubleshoot performance problems on Windows Server 2016 or 2019.
Troubleshooting performance problems requires identifying which resource—CPU, memory, disk, or network—is under stress. On my Windows Server 2022 virtual machine, I used several built-in tools to analyze performance issues. First, I opened Task Manager to quickly check CPU and memory usage. If a process was consuming too many resources, I used Resource Monitor to view detailed statistics for CPU, disk, and network activity. For deeper analysis, I used Performance Monitor, where I added counters like “Processor Time (%)” and “Available MBytes” to track performance trends over time. When the system was slow, I reviewed Event Viewer for warnings or errors related to hardware, services, or applications. I also checked disk health using chkdsk and verified that enough free space was available on the system drive. To optimize performance, I disabled unnecessary startup services and ensured the paging file size was correctly configured. If network performance was slow, I tested throughput using ping and tracert, and verified there were no packet losses. In VMware, allocating more RAM or CPU cores to the virtual machine improved responsiveness. By regularly monitoring and adjusting these parameters, I was able to maintain stable and efficient performance on my Windows Server environment.