25. Role of Windows Firewall in Windows Server and Configuration
Role of Windows Firewall:

Protection: Acts as a barrier between the server and external threats, filtering incoming and outgoing traffic.
Policy Enforcement: Allows administrators to define rules that specify which traffic is permitted or denied.
Logging and Monitoring: Provides logging features to monitor traffic and security events.
Configuration Steps:

Open Windows Firewall: Access via Control Panel > System and Security > Windows Defender Firewall.
Advanced Settings: Click on "Advanced settings" for more granular control.
Inbound/Outbound Rules: Create or modify rules for inbound or outbound traffic.
Right-click on "Inbound Rules" or "Outbound Rules" and select “New Rule”.
Follow the wizard to specify the rule type (e.g., Port, Program, Predefined).
Enable/Disable Rules: Enable or disable rules as needed to control traffic.
Logging: Configure logging options under the properties of Windows Firewall to monitor activity.

26. Network Address Translation (NAT) in Windows Server
NAT Role:

NAT allows a server to act as an intermediary between a private network and the internet, translating private IP addresses to a public IP address.
Configuration Steps:

Install the Routing Role:
Open Server Manager, click on “Add roles and features”, and install the “Routing” role.
Open Routing and Remote Access:
Go to Tools > Routing and Remote Access.
Configure NAT:
Right-click on the server name and select “Configure and Enable Routing and Remote Access”.
Choose the NAT option during the wizard setup.
Add Public and Private Interfaces:
Define the public interface (connected to the internet) and the private interface (connected to the internal network).
Configure NAT Settings: Set NAT properties as needed, and enable the service.

27. Dynamic Host Configuration Protocol (DHCP) Concept and Configuration
DHCP Concept:

DHCP is a network management protocol used to automate the process of assigning IP addresses, subnet masks, gateways, and other network parameters to devices on a network.
Configuration Steps:

Install DHCP Role:
Open Server Manager, click on “Add roles and features”, and install the “DHCP Server” role.
Authorize DHCP Server:
After installation, authorize the DHCP server in Active Directory.
Open DHCP Management Console:
Go to Tools > DHCP.
Create a New Scope:
Right-click on “IPv4” and select “New Scope”.
Follow the wizard to define the scope name, range of IP addresses, subnet mask, and lease duration.
Configure Options:
Set additional options like the default gateway (router) and DNS servers.
Activate Scope: Right-click on the new scope and select “Activate”.

28. Configuring DNS (Domain Name System) in Windows Server
DNS Configuration Process:

Install DNS Role:
Open Server Manager, click on “Add roles and features”, and install the “DNS Server” role.
Open DNS Management Console:
Go to Tools > DNS.
Create a New Zone:
Right-click on “Forward Lookup Zones” and select “New Zone”.
Follow the wizard to choose the zone type (Primary, Secondary, Stub).
Configure Zone Settings: Define the zone name and replication scope.
Add Resource Records:
Right-click on the new zone and select “New Host (A or AAAA)” to add resource records (e.g., hostnames and IP addresses).
Configure Forwarders: Set DNS forwarders for external DNS resolution if needed.

29. Server Manager in Windows Server
Role of Server Manager:

Server Manager is a management console that provides a centralized interface for managing server roles and features.
Usage:

Accessing Server Manager: It opens automatically at login or can be launched from the Start menu.
Dashboard Overview: Provides an overview of server roles, performance, and alerts.
Manage Roles and Features: Use the “Add roles and features” wizard to install new roles.
Remote Server Management: Connect to and manage remote servers from the console.
Monitoring and Reporting: View performance metrics and generate reports on server health.

30. Role of Remote Desktop Services (RDS) in Windows Server 2016/2019

Role of RDS:

RDS allows multiple users to remotely access applications and desktops hosted on a Windows Server.
Configuration Steps:

Install RDS Role:
Open Server Manager, click on “Add roles and features”, and install the “Remote Desktop Services” role.
Use the RDS Deployment Wizard:
After installation, use the wizard to configure the RDS deployment.
Select Deployment Type: Choose whether to deploy a session-based desktop, virtual desktop, or RemoteApp.
Configure Licensing: Set up Remote Desktop Licensing and configure license settings.
Add Session Hosts: Add servers that will host user sessions.
Configure User Access: Define user permissions and configure Remote Desktop Connection settings