MCSA Final Project

1. Project Overview

This project simulates the role of a system administrator in a mid-sized company. The main goal was to build a Windows-based network infrastructure using VMware and Windows Server 2019 that supports 600 users across multiple departments, with centralized services and security policies.

2. Project Objectives

- Install and configure Windows Server 2019.
- Set up Active Directory Domain Services (AD DS) for centralized user management.
- Configure DNS for internal name resolution.
- Deploy DHCP to assign IPs dynamically.
- Implement Group Policy Objects (GPOs) for security and system control.
- Create department-based Organizational Units (OUs).
- Set up File Sharing, Storage Quotas, and Permissions.
- Configure WDS, WSUS, and VPN (RRAS).
- Deploy an Enterprise Certificate Authority (PKI).
- Simulate Windows 10 domain clients and their interaction with infrastructure.

3. Company Structure Design

- The company is divided into 3 departments:
- Sales
- Marketing
- Human Resources (HR)
- Each department includes 200 users.
- Each department has a dedicated IT support user.
- Naming convention: sales1, sales2, …, hr1, mark1, etc.
- Shared Drive Mapping:
- M: → Private for each user
- N: → Shared within the department
- H: → Shared company-wide

4. Virtual Environment Configuration

- Platform: VMware Workstation
- VMs Deployed:
- Windows Server 2019 (Domain Controller)
- Optional: Windows 10 Client for testing
- Network: Host-only, Subnet 192.168.254.0/24

5. Services & Roles Configured

5.1 Active Directory (AD DS)

- Domain: hcompany.local
- OUs created for each department
- Users and groups created with RBAC in mind

5.2 DNS

- Forward Lookup Zone: hcompany.local
- Reverse Lookup Zone: 254.168.192.in-addr.arpa
- Internal sites: site1.hcompany.local, etc.

5.3 DHCP

- Scope created per department
- Reserved IPs for servers
- DHCP Options set for DNS and gateway

5.4 File Server

- Folders created per department
- NTFS and share permissions applied
- Drives mapped via GPO

5.5 Group Policy

- Policies enforced by OU:
- Disable Control Panel, C drive, USB ports
- Set department wallpapers
- AppLocker/Software Restriction Policies
- Print mapping and time-based access

6. Access Control & Security

- First user per department (e.g. sales1) is local admin
- Others are standard users
- EFS used for confidential files
- Password policies:
- Complexity enabled
- 90-day expiration
- 3 failed attempts = lockout

7. Storage Management (FSRM)

- 5GB quota per user
- File screening to block audio/video extensions
- Alerts/logging enabled

8. Additional Services

8.1 WDS (Windows Deployment Services)

- PXE-enabled OS deployment
- Windows 10 image uploaded

8.2 WSUS (Windows Update Services)

- Products: Windows 10, Office
- Automatic approval of updates
- GPO redirects client updates to WSUS

8.3 VPN Server (RRAS)

- Remote access VPN configured
- Domain-based authentication

9. Certificate Authority (PKI)

- Enterprise CA deployed
- Templates created for:
- User Authentication
- Email Encryption
- Digital Signature
- Auto-enrollment via GPO
- CRL and auditing enabled

10. Simulated Windows 10 Client

- Obtains IP from DHCP
- Joins hcompany.local
- GPOs applied: wallpaper, drive mapping, restrictions
- Connects to shared folders and printers
- Uses internal DNS and WSUS
- Receives certificate from CA

11. What I Learned

- How to plan and implement an enterprise-grade infrastructure
- Applying GPOs for real use cases
- Using FSRM, WSUS, WDS, VPN in a corporate setup
- Importance of centralized control, least privilege, and automation
- How different components (AD, DNS, DHCP, CA) work together

12. Conclusion

This project replicates a realistic IT environment using core Microsoft technologies. It reflects the capabilities expected of an MCSA-level system administrator and prepares me to handle real-world enterprise environments.