Milestone 4: Active Directory, LDAP, DNS, DHCP, Group Policies

Technologies Overview:

Active Directory, LDAP, DNS, DHCP, and Group Policies are all technologies commonly used in Windows-based networks to manage network resources, user access, and system configuration.

Here are the objectives of each technology:

1. Active Directory: The primary objective of Active Directory is to provide a centralized authentication and authorization service for Windows-based networks. It enables administrators to manage user accounts, computers, and other network resources from a central location. Active Directory also provides features such as group policy management, software distribution, and security policies.

2. LDAP: LDAP (Lightweight Directory Access Protocol) is a protocol used for accessing and maintaining distributed directory information services over an IP network. Its main objective is to provide a standardized way to access and manage directory services, such as Active Directory.

3. DNS: DNS (Domain Name System) is a protocol used to translate domain names into IP addresses. Its objective is to provide a way to identify and locate resources on a network using human-readable domain names instead of numeric IP addresses.

4. DHCP: DHCP (Dynamic Host Configuration Protocol) is a protocol used to automatically assign IP addresses and network configuration information to devices on a network. Its objective is to simplify network administration by centralizing IP address management and reducing the risk of conflicts and errors.

5. Group Policies: Group Policies are a set of rules that define how computers and users should be configured in a Windows-based network. Their objective is to simplify network administration by enabling administrators to apply consistent settings and configurations across multiple devices and users. Group Policies can be used to manage security settings, network connections, software installation, and many other aspects of system configuration.

Instructions:

Step 1: Active Directory, LDAP

Set up your Windows 2022 Server as a domain controller and use it for AD. You will also need to configure the 2nd Windows 2022 Server as the backup domain controller and AD. All machines should be added to the domain. You should be able to log in to all the VMs using the admin credentials.

Step 2: DNS

Use the VM you designated as a DNS server to set up an internal DNS server. You should also configure your router to point DNS requests toward this server. You can use any DNS solution to create a DNS server on any of the Linux VMs. The DNS server should be able to resolve internal domain names for all the services correctly. For example, if you wanted to access the email server navigating to `mail.sysadmin.local` should allow the user to access and then log in to the mail server.

Step 3: DHCP

All general-use machines should have their IP assigned via DHCP using either the router or Windows Server. All critical services should have their IP statically set.

Step 4: Group Policies

Spicy Cluck Co. currently has 20 employees that will need login access to various systems. See `Milestone 1` for the list of users and their roles in the company. You will have to create different groups based on people's roles and what level of access they should have to various systems.

Step 5: Documentation

Create documentation for each step that would be useful for other sys admins in the future detailing how you set up the different services and any design decisions that you made. You should also include creating, modifying, disabling, and deleting users from the domain and when each one should occur.

Requirements

- [ ] 10 Points - Primary Domain controller is working
- [ ] 10 Points - Backup Domain controller is working
- [ ] 5 Points - AD is set up and the admin user can log in to all systems
- [ ] 10 Points - DNS can resolve internally the:
    - Email Server
    - DNS server
    - Web Server
    - Database Server
    - File Server
    - Primary AD Server
    - Back up AD Server
- [ ] 5 Points - All general machines receive an IP address from DHCP
- [ ] 10 Points - The 20 employees have been assigned to appropriate groups and given permissions
- [ ] 50 Points - Documentation

The lab pass-off will be done with a TA and the documentation should be uploaded to Learning Suite. Documentation must be submitted as a PDF.