Internship Task: Building a Basic Windows Server Active Directory Environment

Scenario Overview:
A company, **TechSphere Ltd.**, is establishing a new branch office and requires an Active Directory setup. As part of your internship, you are tasked to design and implement a basic Active Directory infrastructure, configure network services like DNS and DHCP, and apply basic Group Policies to manage users and devices.

Task Details

Objective:

Set up an Active Directory environment, create basic user and group management, configure essential network services, and apply straightforward Group Policies for security and organization.

Part 1: Setting up Active Directory Domain Services (AD DS)

1. **Domain Controller (DC):**
    - Install and configure Windows Server 2019/2022 on the main server.
    - Promote the server to a Domain Controller.
    - Create a new forest named `techsphere.local`.
    - Verify that the AD DS service is running properly.
2. **Additional Domain Controller (ADC):**
    - Install Windows Server on a secondary server.
    - Join it to the `techsphere.local` domain.
    - Promote it to an Additional Domain Controller to ensure redundancy.

Part 2: DNS and DHCP Configuration

1. **DNS:**
    - Configure DNS zones for `techsphere.local`.
    - Create forward and reverse lookup zones to support name resolution for domain devices.
2. **DHCP:**
    - Install and configure the DHCP role on the DC.

- Set up a scope to assign IP addresses dynamically (e.g., `192.168.1.100-192.168.1.200`).
- Enable DNS dynamic updates for seamless integration.

Part 3: Basic User and Group Management

1. **User Accounts:**
   - Create user accounts for employees (e.g., `John.Doe`, `Jane.Smith`).
   - Use a basic password policy: `Password123` as the initial password (force change on first login).
2. **Security Groups:**
   - Create basic security groups (e.g., `HR_Users`, `IT_Staff`, `Finance_Team`).
   - Assign users to the appropriate groups based on their roles.
3. **Organizational Units (OUs):**
   - Create OUs for departments (e.g., `HR`, `IT`, `Finance`).
   - Place user accounts and computers into the respective OUs.

Part 4: Basic Group Policy Configuration

1. **Password Policy:**
   - Set a simple password policy:
     - Minimum length: 6 characters
     - Complexity: Disabled
     - Expiration: 90 days
2. **Screen Lock Policy:**
   - Enforce a screen lock after 10 minutes of inactivity.
3. **Drive Mapping:**
   - Use Group Policy Preferences to map shared drives:
     - HR: `\\dc\HR_Share`
     - IT: `\\dc\IT_Share`
     - Finance: `\\dc\Finance_Share`
4. **Desktop Background Policy:**
   - Apply a custom desktop background for all users to display the company logo.
5. **User Restrictions:**
   - Disable access to Control Panel and Command Prompt for standard users using Group Policy.

Part 5: Testing and Documentation

1. **Testing:**
    - Create test user accounts in each department and log in from a client computer.
    - Verify:
        - Group Policies are applied correctly.
        - DNS and DHCP are functional.
        - Redundancy through ADC works properly.
2. **Documentation:**
    - Prepare a report including:
        - Steps for configuration of each component.
        - Screenshots of key configurations (e.g., user creation, Group Policies).
        - Results of testing and troubleshooting.