1. Explain User Management and Access Control in Active Directory Environment

Active Directory (AD) is Microsoft's directory service that helps manage users, computers, groups, and network resources. It provides centralized authentication and authorization in a Windows domain environment. User management and access control are two of the most important administrative tasks in any organization.

User Management in AD

User management involves creating, modifying, organizing, and deleting user accounts within the domain. Every user has a **unique account** with login credentials (username and password) that allows them to access the network and its resources.

Creating and Managing Users

Admins can create users manually or in bulk using tools like:

- **Active Directory Users and Computers (ADUC)** – GUI tool.
- **PowerShell** – Command-line scripting for automation.
- **CSV Import** – Bulk user creation with scripts.

Each user account can be customized with:

- Display name
- Email address
- Login script
- Home folder
- Department
- Group membership

Organizational Units (OUs)

Users can be grouped into **OUs** based on departments (e.g., Sales, HR, IT). This makes it easier to apply **Group Policies** or delegate specific admin tasks to junior IT staff without giving full domain control.

Account Policies

Policies help enforce security and operational standards:

- **Password length, history, and complexity**
- **Account lockout after multiple failed attempts**
- **Logon hours (working hours only)**
- **Expiration dates (for interns or contractors)**

Disabling unused or expired accounts is critical to prevent unauthorized access.

Access Control in Active Directory

Access control ensures that only authorized users can access specific files, folders, or systems. It relies on two key components:

1. **Authentication** – Verifying user identity.
2. **Authorization** – Determining what actions the user is allowed to perform.

Permissions and Groups

NTFS Permissions control access at the file system level:

- **Read** – View content only.
- **Write** – Create and modify files.
- **Modify** – Read, write, delete.
- **Full Control** – All actions.

Security Groups

Instead of assigning permissions to each user, admins assign users to **groups** (e.g., HRGroup, ITAdmins), then apply permissions to the group.

Types of groups:

- **Security Groups** – For access control.
- **Distribution Groups** – For email purposes (not used for permissions).

This method simplifies permission management, especially when employees join or leave departments.

Auditing and Monitoring

Admins can enable **auditing policies** to track access to sensitive files. Logs are stored in the Event Viewer and help detect suspicious activity.

Best Practices

- Use **Group-Based Access Control (GBAC)**.
- Disable inactive accounts quickly.
- Apply the **Principle of Least Privilege**.
- Use strong password and lockout policies.
- Document group memberships and access rights.
- Periodically audit users and their permissions.

With well-managed user accounts and access control in Active Directory, organizations can reduce the risk of data breaches and improve productivity.

2. Explain Group Policy Management with Example

Group Policy is a feature in Windows that allows centralized control over user and computer settings within an Active Directory domain. It helps administrators manage and enforce specific configurations across multiple users and machines without manual work.

Group Policy Objects (GPOs)

A **Group Policy Object (GPO)** is a set of rules and settings that can be linked to:

- **Sites** (e.g., branch locations)
- **Domains** (entire organization)
- **OUs** (departments like HR, Sales)

GPOs can configure settings under two main sections:

- **Computer Configuration**: Applies to computers.
- **User Configuration**: Applies to users.

Common Uses of Group Policy

- Enforce strong password policies.
- Redirect user folders (e.g., Documents) to network drives.
- Disable USB ports.
- Restrict access to certain Control Panel options.
- Set custom desktop wallpapers.

- Automatically install software.

How GPOs Are Processed

GPOs are applied in this order:

1. **Local Group Policy**
2. **Site GPOs**
3. **Domain GPOs**
4. **OU GPOs**

The last GPO to apply (usually OU) has the highest priority in case of conflict. This is called the **LSDOU** order.

Example: Enforce Screen Lock After Inactivity

Objective: Lock all computers if idle for 10 minutes.

Steps:

1. Open **Group Policy Management Console (GPMC)**.
2. Create a new GPO called “Screen Lock Policy”.
3. Edit the GPO:
    a. Navigate to:
    User Configuration > Administrative Templates > Control Panel > Personalization
    b. Enable: "Screen saver timeout" (600 seconds)
    c. Enable: "Password protect the screen saver"
4. Link the GPO to the target OU (e.g., "AllEmployees").

All users in that OU will have auto-lock enforced.

Advanced Group Policy Features

- **Security Filtering**: Apply GPO to a specific user or group only.
- **WMI Filtering**: Apply GPO based on hardware/software conditions (e.g., apply only to laptops).
- **Loopback Processing**: Useful in kiosk or shared computer setups where the user policy should depend on the machine.

Monitoring and Troubleshooting

- Use **gpresult** or **Resultant Set of Policy (RSoP)** to see effective GPOs.

- Run **gpupdate /force** to refresh policy settings instantly.

Best Practices

- Use descriptive GPO names.
- Organize GPOs by function (e.g., Security, Desktop, Software).
- Test GPOs in a small OU before wide deployment.
- Limit the number of GPOs per OU to avoid slow login times.
- Document each GPO and its purpose.
- Backup GPOs using GPMC.

Group Policy is a powerful and flexible tool that helps enforce organizational standards across the network with minimal manual effort.

3. Explain Backup and Disaster Recovery Strategy for Enterprise Servers

In enterprise environments, **backup and disaster recovery (DR)** are critical for data protection, system resilience, and business continuity. Servers host essential services like databases, websites, applications, and shared files, so their protection is a top IT priority.

What Is a Backup?

A **backup** is a copy of data stored separately from the original, which can be used to restore systems or files in case of:

- Hardware failure
- Cyberattacks (e.g., ransomware)
- Human error (accidental deletion)
- Natural disasters (fire, floods)

Types of Backups

1. **Full Backup**: Backs up everything. Time-consuming and storage-heavy but easy to restore.
2. **Incremental Backup**: Backs up only data changed since the last backup (faster, saves space).

3. **Differential Backup**: Backs up changes since the last **full** backup (quicker to restore than incremental).

Example:

- Sunday: Full Backup
- Monday to Saturday: Incremental Backups
  This ensures daily protection with lower storage use.

Backup Storage Options

- **Local storage**: External drives, backup servers (quick access but vulnerable).
- **Network-attached storage (NAS)**: Shared storage in the organization.
- **Cloud Backup**: Azure, AWS, Google Cloud (offsite and secure).
- **Tape backup**: Long-term archiving, used in large enterprises.

3-2-1 Backup Strategy

A widely recommended method:

- **3 copies** of data (1 primary + 2 backups)
- **2 types** of media (e.g., hard disk + cloud)
- **1 copy** offsite (cloud or remote location)

What Is Disaster Recovery (DR)?

Disaster Recovery is a broader strategy than backup. It includes:

- Steps to restore servers, apps, and data after a crisis
- Recovery sites (physical or virtual)
- A clear, documented plan

Key Concepts in DR

- **RTO (Recovery Time Objective)**: Maximum time allowed for restoring service.
- **RPO (Recovery Point Objective)**: How much recent data loss is acceptable (e.g., last 1 hour of changes).

Example: A company with an RTO of 4 hours and an RPO of 15 minutes must resume systems within 4 hours and tolerate losing only 15 minutes of data.

DR Plan Components

- Inventory of systems and data
- Contact lists and communication plan
- Step-by-step recovery procedures
- Alternative infrastructure (cloud VMs, offsite servers)
- Regular testing and updates

Backup and DR Tools

- **Windows Server Backup**
- **Veeam Backup & Replication**
- **Acronis Backup**
- **Azure Backup**
- **Symantec NetBackup**

These tools automate backups, test restore procedures, and send alerts on success/failure.

Testing the Plan

A DR plan is only effective if it’s tested:

- Perform mock disasters every 6 months
- Simulate server failures or ransomware attacks
- Verify backup integrity and restore time

Best Practices

- Schedule regular backups (daily, weekly, monthly).
- Encrypt backup data to prevent leaks.
- Store one backup copy offline or offsite.
- Keep backup servers secured and access-restricted.
- Maintain logs of backup activities.
- Test restores monthly.

Backup and disaster recovery are not just technical processes—they are business-critical strategies that protect an organization's reputation, data, and services.

4. Explain File Server Management and Configuration

A **file server** is a centralized server that stores files for multiple users on a network. It enables sharing, collaboration, secure storage, and data organization. Proper configuration ensures that users can access what they need while preventing unauthorized access.

What a File Server Does

- Hosts shared folders (e.g., \Server\HR)
- Allows file access over LAN/WAN
- Controls who can read, write, or modify files
- Provides data for backup and audit

Steps to Set Up a File Server

1. **Install File Server Role**:
    a. Use Server Manager > Add Roles and Features
    b. Select “File and Storage Services” > “File Server”
2. **Create Shared Folders**:
    a. Example: D:\Shared\Finance
    b. Right-click > Properties > Sharing tab > Share
3. **Set Permissions**:
    a. **NTFS Permissions** (more detailed, apply to files/folders)
    b. **Share Permissions** (apply when accessed over network)
4. **Assign Permissions to Groups**:
    a. Use security groups like “HR_Team” or “Finance_Managers”
    b. Apply permissions like Read, Modify, Full Control

Permission Levels

- **Read**: View contents
- **Write**: Add or modify
- **Modify**: Read/write/delete
- **Full Control**: Everything, including changing permissions

Best Practices for Permissions

- Always assign to **groups**, not individual users.
- Use **least privilege**—only give necessary access.

- Avoid giving Full Control unless required.
- Document folder structures and permissions.

Advanced Features

- **Access-Based Enumeration (ABE)**: Hides folders a user doesn't have permission to access.
- **Shadow Copies**: Allows restoring older versions of files.
- **File Server Resource Manager (FSRM)**: Adds quotas, screens, reports.
    - Block file types (e.g., MP3, EXE)
    - Limit storage per user or folder
    - Send alerts on space usage

Example Configuration

Company creates:

- \\Server\Projects shared folder
- Groups: "Designers", "Managers"
- Permissions:
    - Designers: Modify
    - Managers: Full Control

Only the right people can access, edit, or manage project files.

Monitoring and Logging

- Enable file access auditing in GPO or local policy
- Monitor who accessed or deleted files
- Use Event Viewer for logs

Security Measures

- Enable firewalls and antivirus on the server
- Restrict share access to internal networks
- Disable guest access
- Apply regular Windows updates

Maintenance

- Review folder permissions monthly

- Clean up unused files
- Monitor disk usage
- Backup important folders regularly

A well-managed file server enhances teamwork, secures sensitive information, and makes file access smooth for employees across departments.