🏢 Active Directory Containers and GPOs

In a Windows Server environment (e.g., Server 2016), when an organization sets up a domain like `class.com`, it can use **Active Directory (AD)** to manage and organize network resources.

Within AD, there are **containers** that help structure the domain:

- **Domains**: The highest-level boundary for policies and authentication.
- **Sites**: Groupings based on physical/geographic locations.
- **Organizational Units (OUs)**: Logical containers used to organize users, groups, and computers.

Each of these containers can hold:

- **Users**
- **Groups**
- **Computers**

And can be targets for **Group Policy Objects (GPOs)**, which define security settings, software installations, scripts, and user environment configurations.

🧠 Understanding GPO (Group Policy Object)

A **Group Policy Object (GPO)** is a collection of settings applied to users or computers. GPOs allow IT administrators to:

- Enforce desktop configurations.
- Restrict or allow access to features (e.g., Control Panel).
- Deploy software.
- Run scripts at startup or login.

There are two main types:

1. Local GPO

- Exists on individual machines.
- Used when the system is not part of a domain or when a quick, machine-specific policy is needed.
- Example: On Windows 10/11, use a local GPO to block access to the Control Panel.

2. Domain GPO

- Created and managed via Active Directory.
- Applied across many users and machines in a domain.
- Managed centrally and linked to containers like OUs.
- Enforced through ADDS (Active Directory Domain Services).

🔗 How GPOs are Applied Across AD

When a user (e.g., `User1`, `User2`) logs in from their **Client-PC**, the Domain GPOs are applied based on their container hierarchy in Active Directory.

GPOs are processed in the following order (known as **GPO Precedence**):

1. **Local GPO**
2. **Site-level GPOs**
3. **Domain-level GPOs**
4. **OU-level GPOs** (including nested OUs)

If multiple GPOs have conflicting settings, the **last applied** (closest to the object in the hierarchy) typically takes effect—**unless enforced**.

⚙️ GPO Services and Functions

Here are some critical management functions and tools related to GPOs:

✅ What is GPO?

A framework to manage configurations for users and computers in an AD environment, enforcing IT policy across the domain.

🥇 GPO Precedence

Controls which GPO takes effect when multiple policies apply. Closer GPOs (e.g., OU) override broader ones (e.g., domain) unless otherwise specified.

🚫 Block Inheritance / Enforced

- **Block Inheritance**: Prevents GPOs from higher containers from applying to a lower container like an OU.
- **Enforced**: Forces a GPO to apply even if the target container blocks inheritance.

🧪 WMI Filter

WMI (Windows Management Instrumentation) filters allow GPOs to apply based on dynamic system conditions, such as:

- OS version
- Amount of RAM
- System type

Useful for targeting GPOs only to machines meeting certain criteria.

💾 GPO Backup and Restore

Administrators can back up GPOs to preserve configurations and restore them when needed. This is essential for disaster recovery or duplicating settings across environments.

💻 GPO Commands

Useful tools include:

- `gpupdate /force`: Forces an immediate policy refresh.
- `gpresult /r`: Displays Resultant Set of Policy (RSoP) for a user or computer.

- PowerShell cmdlets:
    - `Get-GPO`, `Backup-GPO`, `Restore-GPO`, `New-GPO`, etc., used to script and automate GPO management.

🧩 Final Summary

GPOs are at the heart of policy management in Windows Server environments. By leveraging containers like Domains, Sites, and OUs in AD, administrators can apply different configurations to users and machines—ensuring centralized, scalable, and secure management. Features like precedence, WMI filters, inheritance control, and powerful command-line tools make GPOs extremely flexible and powerful in enterprise settings.

🧪 Lab Setup: Apply a Domain GPO to Block Control Panel Access

🖥️ Environment Requirements

- **1 Domain Controller** (Windows Server 2016 or later, e.g. `DC01.class.com`)
- **1 Client Machine** (Windows 10/11, domain-joined)
- AD DS (Active Directory Domain Services) and Group Policy Management Console (GPMC) installed on the server

✅ Step-by-Step Process

🔹 1. Setup Active Directory (One-time Setup)

1. Promote the Windows Server to a **Domain Controller**.
2. Create a domain (e.g. `class.com`).
3. Install **Group Policy Management Console**:
    - Open **Server Manager** > Add Roles and Features > Features > Check **GPMC**.

🔹 2. Create Organizational Units (OUs) and Users

1. Open **Active Directory Users and Computers (ADUC)**.
2. Create an OU: e.g., `StudentsOU`.
3. Inside that OU, create test users: `user1`, `user2`.
4. Create a **security group** if needed and add users.

🔹 3. Join Client PC to the Domain

1. On Windows 10/11 client:
    - System > About > Rename this PC (Advanced) > Join domain: `class.com`
    - Enter credentials of a domain admin.
    - Reboot.

🔹 4. Create and Link a GPO

1. Open **Group Policy Management Console (GPMC)** on the server.
2. Right-click your OU (`StudentsOU`) > **Create a GPO in this domain and Link it here...**
    - Name it: `BlockControlPanelGPO`.
3. Right-click the new GPO > **Edit**.

🔹 5. Configure the GPO to Block Control Panel

Navigate to:

mathematica

```
User Configuration > Administrative Templates > Control Panel >
Prohibit access to Control Panel and PC settings
```

1. Double-click and set it to **Enabled**.
2. Close the editor.

🔹 6. Test the Policy

1. Log into the client machine as `user1`.

Open Command Prompt and run:

bash
```
gpupdate /force
```

2.
3. Try to open Control Panel — it should be **blocked**.

🔹 7. Use GPO Tools to Verify

On the client, run:

bash

```
gpresult /r
```

Check if `BlockControlPanelGPO` is listed under **Applied Group Policy Objects**.

🛠️ Optional Enhancements

- **WMI Filter**: Apply GPO only if the client is Windows 11:

In GPMC > WMI Filters > New > Use query like:

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.%" AND
ProductType="1"
```

    -

- **GPO Backup**:
    - In GPMC > Right-click GPO > Backup
- **Use PowerShell**:
    - `New-GPO -Name "BlockControlPanelGPO"`
    - `Set-GPLink -Name "BlockControlPanelGPO" -Target "OU=StudentsOU,DC=class,DC=com"`