Group Policy Objects

TABLE OF CONTENTS

01
What is a GPO?

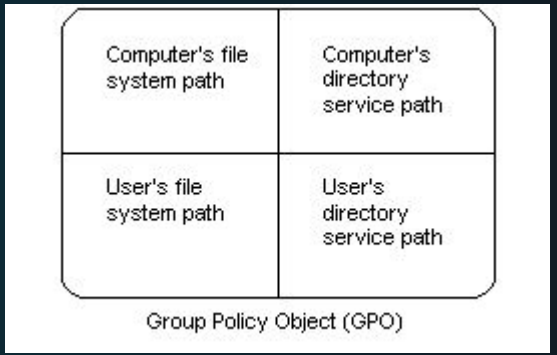
Structure, function, purpose

GPO – GROUP POLICY OBJECT

A Group Policy Object (GPO) is a virtual collection of policy settings. A GPO has a unique name, such as a GUID.

Group Policy settings are contained in a GPO. A GPO can represent policy settings in the file system and in the Active Directory. GPO settings are evaluated by clients using the hierarchical nature of Active Directory.

Structure of a GPO



WHAT DOES GROUP POLICY DO?

POLICIES

Group policy is a collection of policies defined as registry keys and values. These keys and values are stored in a GPO, or group policy object, in a format that can be easily changed or transferred on different computers.

ENFORCEMENT

GPOs through Active Directory have the ability to change and modify policies of all computer on that network. The AD Domain Controller be polled and the appropriate settings will be enforced through the specified GPOs

A GPO's OPERATION

ENFORCEMENT

Group Policy is processed in the following order:

1. LOCAL
2. SITE
3. DOMAIN
4. OU

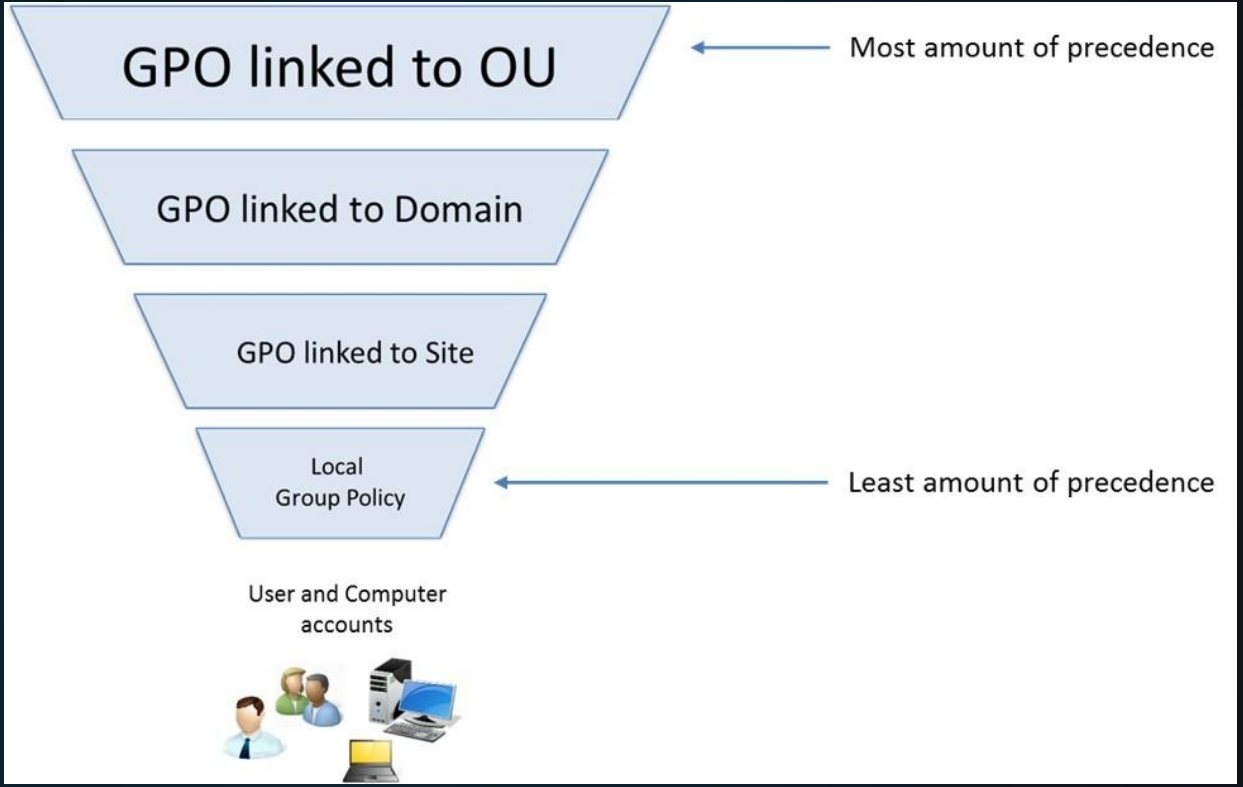
INHERITANCE

Where a Group Policy Preference Settings is configured and there is also an equivalent Group Policy Setting configured, then the value of the Group Policy Setting will take precedence. This can be blocked or enforced for specific policies at each level

FILTERING

WMI filters allow administrators to apply the GPO only to, for example, computers of specific models, RAM, installed software, or anything available via WMI queries.

GPO Hierarchy



02

What uses a GPO?

Access, Retrieval

LOCAL GROUP POLICY CONSOLE

The local group policy console is accessible on all Windows machines and manages the settings for the local-level group policy. These policy changes are at the lowest level and will be overridden by any higher-level policies

This console can be accessed through MMC or gpedit.msc

GROUP POLICY MANAGEMENT CONSOLE

The group policy management console manages higher level GPOs and can send out GPOs to computers on the domain overriding any local policies if an overlap occurs.

This console can be accessed through MMC or gpmc.msc

THERE ARE 2 SEPARATE GUI METHODS OF ACCESSING GPOS

COMMAND LINE METHODS

POWERSHELL

Powershell methods are only accessible on Active Directory workstation using the X-GPO set of commands.

SECEDIT

In chapter 9, we briefly covered over secedit. Secedit is a command line tool that analyzes and determines security templates on the local computer. This does not analyze the complete LGPO though.

REGISTRY

ALL changes to policies, regardless of level, will be reflected in a change in the registry. Edit and manipulate registry keys at your own risk.

Group Policy Module

(Get, New, Set, Remove, Copy) -GPO

Does it's respective tasks as seen before for a Group Policy Object

Backup-GPO

Backs up one or all GPOs on a domain

Get-GPOReport

Generates a report either in XML or HTML format for a specified GPO or for all GPOs in a domain.

(Get, Remove, Set) -GPRegistryValue

A GPRegistryValue is a value in the registry under the Computer Configuration or User Configuration in the GPO

Import-GPO

Imports the Group Policy settings from a backed-up GPO into a specified GPO.

Invoke-GPUpdate

Schedules a remote Group Policy refresh on the specified computer.

LGPO.exe

An external application designed by Microsoft to easily import, export, and transfer GPOs to computers that are not on a domain.

https://www.microsoft.com/en-us/download/details.aspx?id=55319

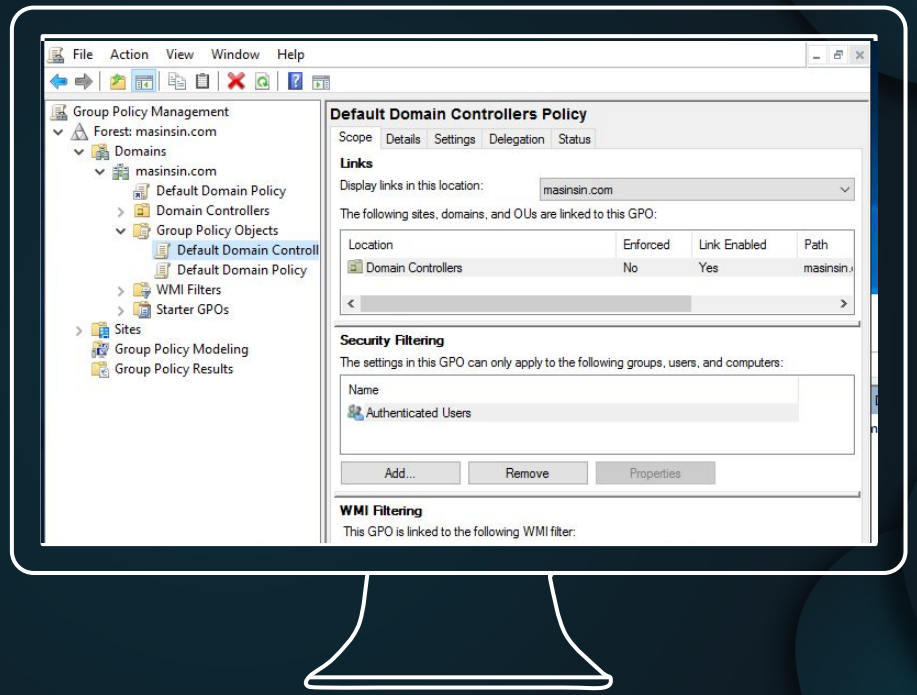
03

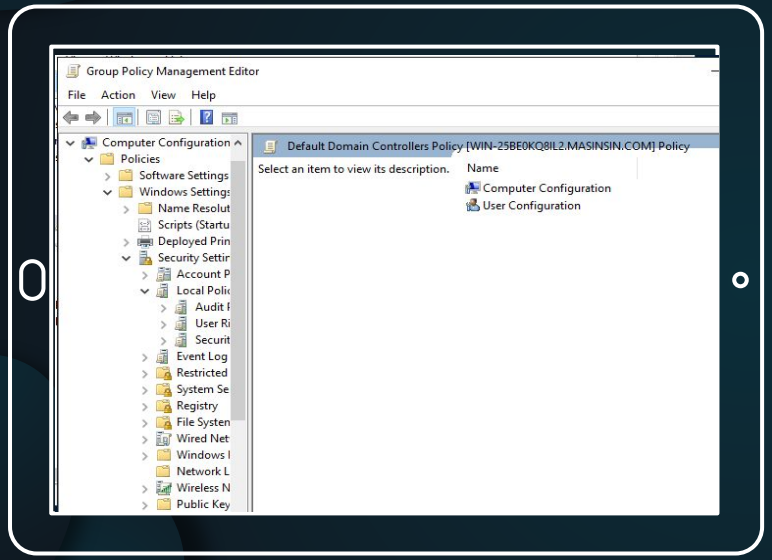
CHANGING GPOs

Modifying values of a GPO

GROUP POLICY MANAGEMENT CONSOLE

Select a GPO from one on the domain and edit policies. You can also change whether the GPO is enforced or not.





GROUP POLICY

Change and edit individual policy settings here.

04

Where to find GPOs

STIGs and the like

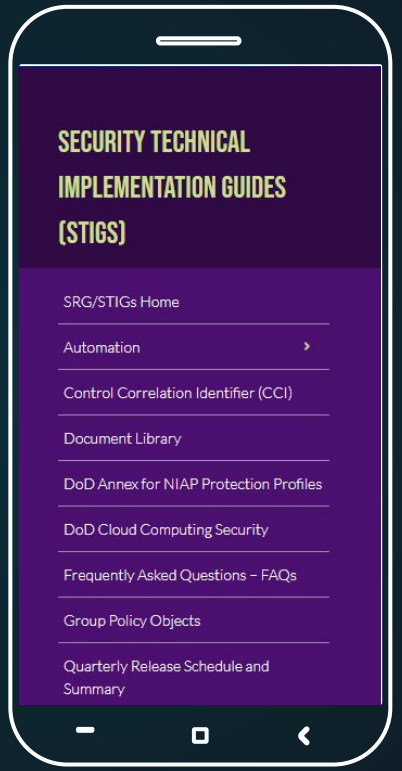
STIGs

Security Technical Implementation Guides or STIGs are guidelines to follow when creating security policies for your network

Department of Defense

The Department of Defense (DoD) has free pre implemented Group Policy STIGs that follow modern and up-to-date security policies.

https://public.cyber.mil/stigs/gpo/



THANKS!

Does anyone have any questions?