

Lab #008

Group Policy Maintenance and Troubleshooting: Comments, reports, and write-ups

Eric Webb and Jon Martin

Learning Objective: Document, search, and troubleshoot group policy.

Equipment: No new equipment is required.

Notes: We added comments to our control panel gpo and exported a report from it. We also set up the central store, as well as play around with filter options.

Diagrams:

no control panel 4 u

Data collected on: 4/20/2020 5:40:26

show all

hide

Details

hide

Domain	domain1.local		
Owner	DOMAIN1\Domain Admins		
Created	4/1/2020 5:10:06 PM		
Modified	4/1/2020 5:16:10 PM		
User Reviews	2 (AD), 0 (SYSVOL)		
Computer Reviews	0 (AD), 0 (SYSVOL)		
Unique ID	{D9B8A9F5-100D-48F7-B1B9-8701B071873F}		
GPO Status	Enabled		

Links

hide

Location	Enforced	Link Status	Path
Main	No	Enabled	domain1.local/Main

This list only includes links in the domain of the GPO.

Security Filtering

hide

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation

hide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
DOMAIN1\Domain Admins	Edit settings, delete, modify security	No
DOMAIN1\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

hide

No settings defined.

User Configuration (Enabled)

hide

Policies

hide

Administrative Templates

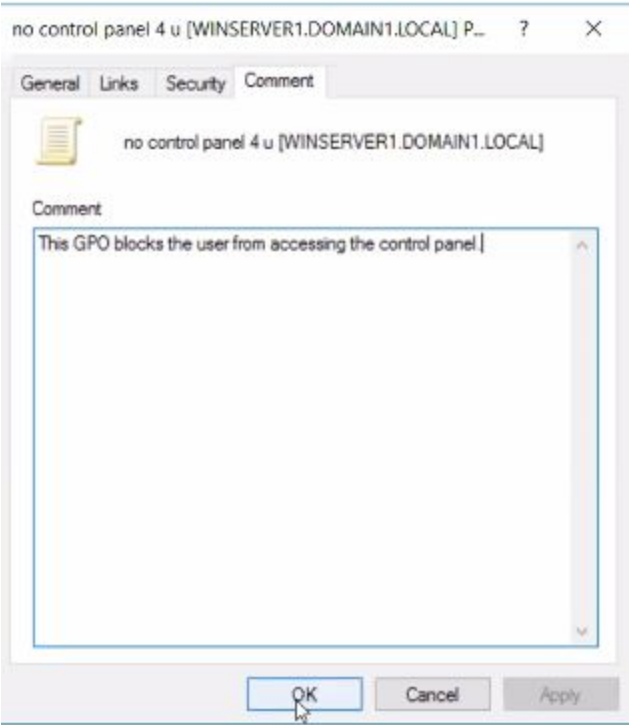
hide

Policy definitions (.ADML files) retrieved from the local computer.

Control Panel

show

Central Store



GPO Comment

no control panel 4 u

Created on: 4/20/2020 5:40:26

show all

hide

Details

Domain	domain1.local		
Owner	DOMAIN1\Domain Admins		
Created	4/1/2020 5:10:08 PM		
Modified	4/1/2020 5:18:16 PM		
User Restrictions	2 (AD), 0 (SYSTEM)		
Computer Restrictions	0 (AD), 0 (SYSTEM)		
Unique ID	{D9B8A9F5-100D-4087-B18F-8701B017187F}		
GPO Status	Enabled		

hide

Links

Location	Enforced	Link Status	Path
Main	No	Enabled	domain1.local/Main

This list only includes links in the domain of this GPO.

hide

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name	
NT AUTHORITY\Authenticated Users	

hide

Delegation

These groups and users have the specified permissions for this GPO

Name	Allowed Permissions	Inherited
DOMAIN1\Domain Admins	Edit settings, delete, modify security	No
DOMAIN1\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

hide

Computer Configuration (Enabled)

No settings defined

hide

User Configuration (Enabled)

hide

Policies

Administrative Templates

Policy definitions (ADM/OC files) retrieved from the local computer

hide

Control Panel

show

Exported gpo report

References: Only the book provided, Mastering Windows Group Policy.

Questions: Keeping gpos simple and easy to understand means easy granting and revoking of permissions. Initials/name, what it does, and who it was made for. GPO reports are really good for backups, as well as just having a copy on hand. You could also share the gpo with other sys admins. There are lots of GPOs in an enterprise environment, and good naming conventions make finding and changing settings much much easier. It allows you to filter by comments, so good comments help too. Setting up starting GPOs is a good way to help junior developers and hand off the work while keeping the critical settings set. Backing up GPOs is a good way to fix if someone deletes the gpo on accident, or to go to a previous version of the gpo. The central store is a place to put adml/admx files once, and then these settings get distributed to domain controllers. Gpupdate forces a group policy update to happen, instead of waiting up to 90 minutes. Running gpresult shows the different permissions between typical users and administrators. There shouldn't be a change in the computers section, as they are the same computer. Group Policy Modeling shows what your changes will do.

Conclusion: Lots of helpful troubleshooting techniques. I imagine they will be very helpful for the case study.