Consolidating Group Policy, part 1: Get-GpoReport and Advanced Group Policy Management (AGMC)

4sysops.com/archives/consolidating-group-policy-part-1-get-gporeport-and-advanced-group-policy-management

James Rankin Wed, Aug 18 2021 group policy 1

In this series of three posts, I will discuss various tools that allow you to manage and consolidate your Group Policy environment. In today's article, I will make some general remarks and take a look at two useful GPO tools: Get-GpoReport and Advanced Group Policy Management.

Contents

1. Preparation
2. Get-GpoReport
3. Advanced Group Policy Management

- Author
- Recent Posts

James Rankin

James is a consultant from the UK, specializing mainly in end-user computing, Active Directory and client-side monitoring. When not consulting for james-rankin.com, he can often be found blogging, writing technical articles and speaking at conferences and user groups.

Many enterprises rely heavily on Group Policy to provide configuration settings to their users and devices. Group Policy, despite being relatively unchanged since 2006, encompasses many configuration items that can be used to push granular settings down to domain-joined devices and/or users. Enterprises often have very complicated Group Policy implementations, which only become more complicated when multiple forests/domains and/or mergers and acquisitions are factored into the equation. In many instances, the complexity of GPO implementation, combined with the fear of inadvertently impacting the user base, leads to Group Policy being left in a sprawling, bloated state that becomes increasingly difficult to manage or unpick.

Microsoft's longer-term goal is to move away from Group Policy toward what they call "modern management"—using technology such as InTune and Desired State Configuration rather than the legacy GPO methods to manage their user and device base. For the short term, however, Group Policy is here to stay, at the very least in a hybrid way. As part of a migration away from Group Policy, or just to simplify the day-to-day management and overhead, a consolidation and remediation exercise such as that described in this article is vital.

As well as making management easier and migration more of a realistic possibility, this exercise can also make the processing of policies more efficient, simply by removing unneeded or inapplicable configuration items.

Preparation

If you're in an environment with a sizable number of GPOs (or even if you're not), you may well want to automate as much of this as possible. Trawling through Group Policy Objects manually is a thankless, time-consuming task, so we will suggest automated ways to find the information wherever possible.

With regard to what we'd like to get out of the GPO consolidation exercise, we will attack it from these angles:

- Remove broken GPOs and dead links
- Remove disabled GPOs
- Remove unlinked GPOs
- Remove empty GPOs
- Identify GPOs with no content
- Identify GPOs with incorrect permissions
- Identify GPOs with inapplicable or legacy settings
- Identify GPOs with invalid security filters

Make sure that the user account you are using to do the consolidation exercise has at least Read permissions to all the GPOs in your forest(s) or domain(s).

For the Group Policy PowerShell cmdlets, you need to have access to a machine with the Remote Server Administration Tools (RSAT) installed.

Ensure that you have a backup of your GPOs. Even though we are going through a "read-only" exercise and parsing the data, prudence suggests that you should have a full backup, just in case. You can perform the backup either manually from GPMC by using the "Back Up" or "Save Report" context menu functionality, or use the *Backup-Gpo* cmdlet (which allows all GPOs in a domain to be backed up at once).
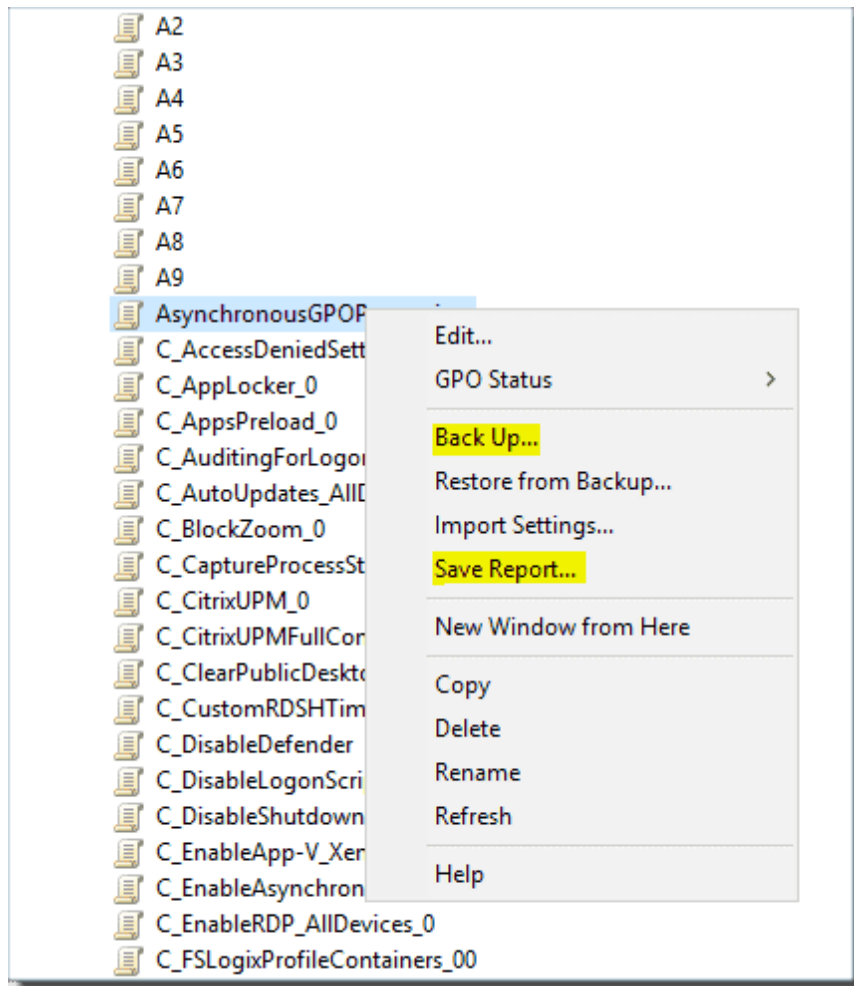
Backing up GPOs

There are a couple of tools that can be used for outputting GPO data. The go-to tool is usually the Group Policy PowerShell cmdlets, mainly Get-GpoReport. This can output either HTML or XML reports for all GPOs in a domain. You can combine this with other cmdlets, such as Get-GPPermission and Get-GPO, to produce more targeted data.

Get-GpoReport

One main issue with Get-GpoReport, however, is that it often fails to output an HTML report successfully when run on a large number of policy objects. The XML report works fine; however, this is considerably less readable than the HTML report. Also, even if the HTML report works, parsing this information into actionable data can be time-consuming and may require further scripted manipulation.

Advanced Group Policy Management

Advanced Group Policy Management Console (AGPMC) is a free tool from Microsoft that extends the capabilities of the "standard" GPMC. It adds features such as change control, locking, check in/out, labeling, archiving, etc. This added functionality is vital to enterprises looking to achieve greater control of their Group Policy implementations.

AGPM version 4.0 SP3 is the recommended version for environments covering Windows 7/2008 up to Windows 10/2019.
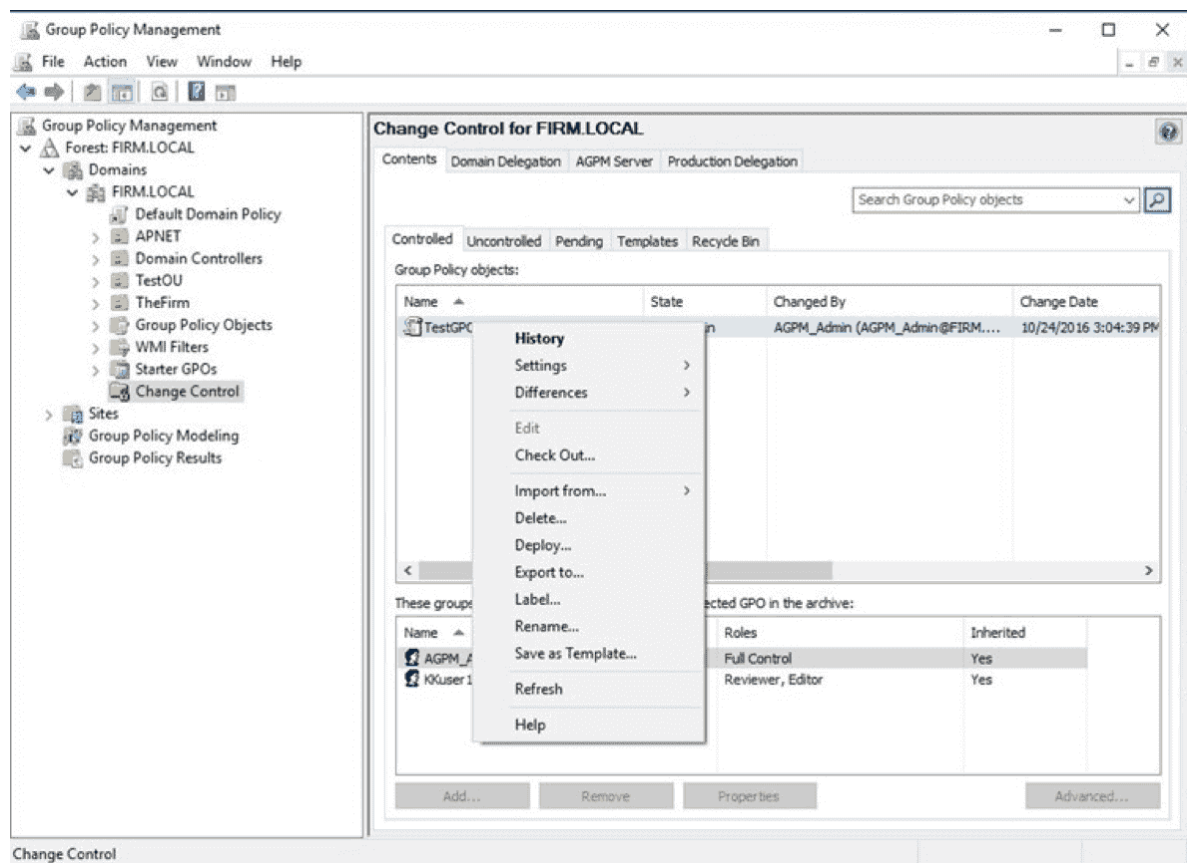
AGPM

The implementation of AGPMC will provide far more control and failsafes than are currently available within a typical enterprise environment where they use the standard GPMC, as well as allowing more granular reporting and assessment. These changes are crucial to improving the ongoing management of the GP estate.

AGPM simply requires dedicated service accounts and an installation of the console to be implemented.

It is also recommended that the editing of GPOs be locked to AGPMC to prevent users from accessing the policies from other instances of the Group Policy console. If you aren't already using AGPMC, you should start as soon as possible.

In my next article, I will explain how to deal with GPOs that are broken, disabled, invalid, or inapplicable.