Consolidating Group Policy, part 2: GPOZaurr

4sysops.com/archives/consolidating-group-policy-part-2-gpozaurr

August 19, 2021

James Rankin Thu, Aug 19 2021 group policy, active directory 0

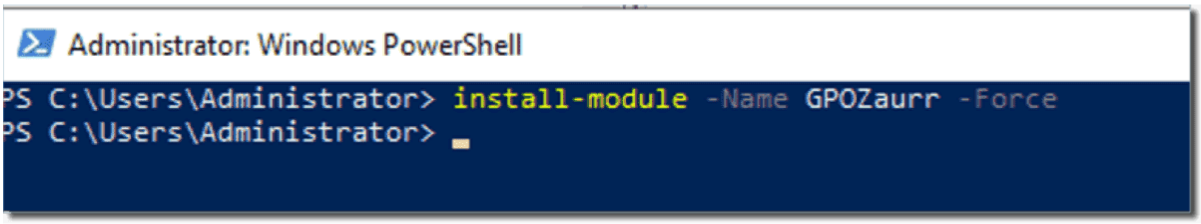
GPOZaurr from Evotec IT is a PowerShell module that is very useful for consolidating and managing Group Policy. In this post, I will demonstrate how you can use GPOZaurr to create Group Policy reports and deal with broken, disabled, invalid, or inapplicable GPOs. This is the second post in my series about Group Policy consolidation.

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.

Installing GPOZaurr

You need RSAT installed to support GPOZaurr; after that, you can simply add the module from PowerShell.

Install-Module -Name GPOZaurr -Force



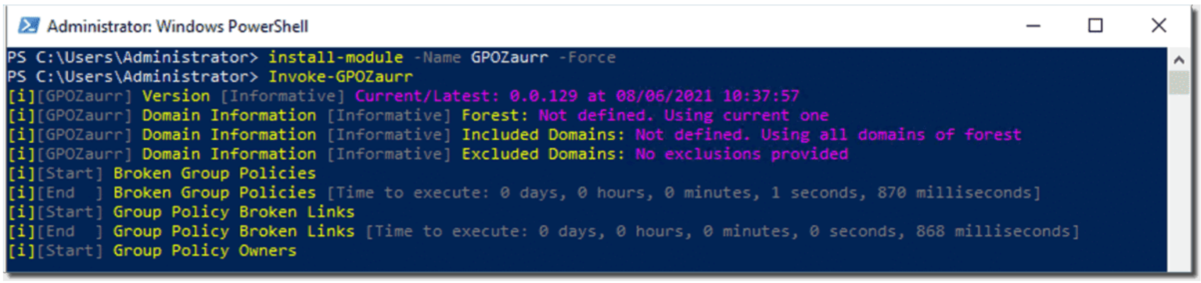
```
PS C:\Users\Administrator> install-module -Name GPOZaurr -Force
PS C:\Users\Administrator> _
```

Install GPOZaurr

If you're unable to contact the PowerShell gallery, then you can download the modules on a separate workstation and copy them to the target before installing the module.

Full details are provided on GitHub and in this blog post as well.

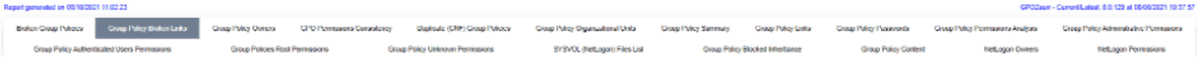
The module has many reports that you can use, which are laid out in the second link above. However, in most cases, you can simply generate a full report by running Invoke-GPOZaurr.



```
PS C:\Users\Administrator> install-module -Name GPOZaurr -Force
PS C:\Users\Administrator> Invoke-GPOZaurr
[i][GPOZaurr] Version [Informative] Current/Latest: 0.0.129 at 08/06/2021 10:37:57
[i][GPOZaurr] Domain Information [Informative] Forest: Not defined. Using current one
[i][GPOZaurr] Domain Information [Informative] Included Domains: Not defined. Using all domains of forest
[i][GPOZaurr] Domain Information [Informative] Excluded Domains: No exclusions provided
[i][Start] Broken Group Policies
[i][End  ] Broken Group Policies [Time to execute: 0 days, 0 hours, 0 minutes, 1 seconds, 870 milliseconds]
[i][Start] Group Policy Broken Links
[i][End  ] Group Policy Broken Links [Time to execute: 0 days, 0 hours, 0 minutes, 0 seconds, 868 milliseconds]
[i][Start] Group Policy Owners
```

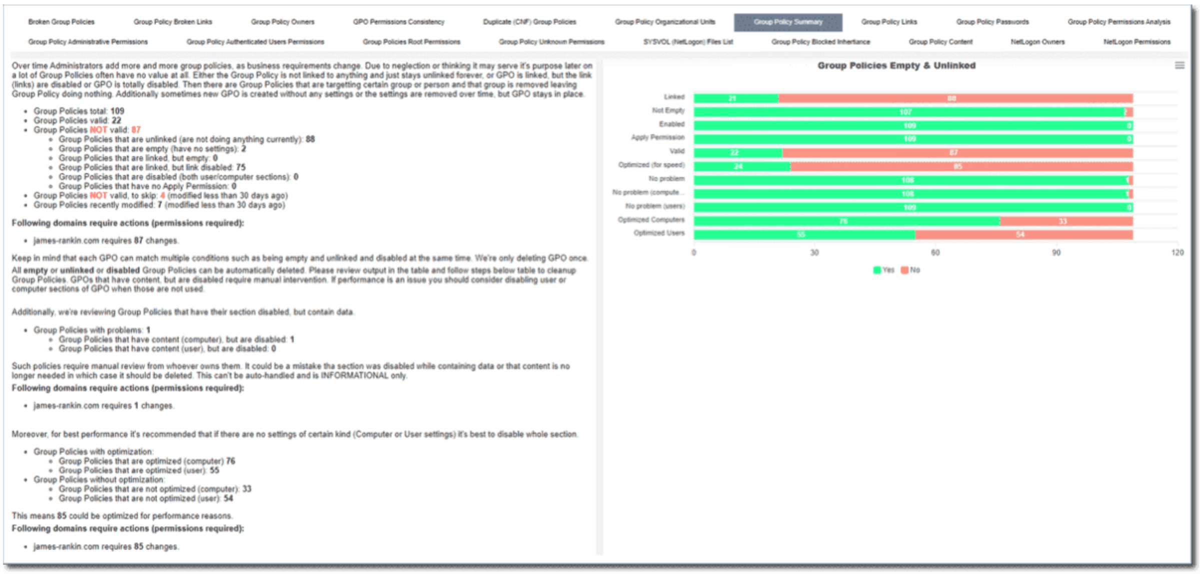
Generating reports

Once the command has finished executing, an interactive HTML report will be generated. This has many output sections that can be browsed, each of which provides different data sets. Each tabbed section is shown below.


Report generated on 05/10/2021 11:02:23
GPOZaurr - Current/Latest: 0.0.123 at 08/06/2021 10:37:57
Broken Group Policies
Group Policy Broken Links
Group Policy Owners
GPO Permissions Consistency
Duplicate (CNF) Group Policies
Group Policy Organizational Units
Group Policy Summary
Group Policy Links
Group Policy Passwords
Group Policy Permissions Analysis
Group Policy Administrative Permissions
Group Policy Authenticated Users Permissions
Group Policies Root Permissions
Group Policy Unknown Permissions
SYSVOL (NetLogon) Files List
Group Policy Blocked Inheritance
Group Policy Content
NetLogon Owners
NetLogon Permissions

GPOZaurr report sections

There is also a "Summary" section that provides a handy overview of the report and its recommendations.


Broken Group Policies
Group Policy Broken Links
Group Policy Owners
GPO Permissions Consistency
Duplicate (CNF) Group Policies
Group Policy Organizational Units
Group Policy Summary
Group Policy Links
Group Policy Passwords
Group Policy Permissions Analysis
Group Policy Administrative Permissions
Group Policy Authenticated Users Permissions
Group Policies Root Permissions
Group Policy Unknown Permissions
SYSVOL (NetLogon) Files List
Group Policy Blocked Inheritance
Group Policy Content
NetLogon Owners
NetLogon Permissions
Group Policies Empty & Unlinked
Linked 21 88
Not Empty 107 2
Enabled 109 0
Apply Permission 109 0
Valid 22 87
Optimized (for speed) 24 85
No problem 108 1
No problem (compute... 108 1
No problem (users) 109 0
Optimized Computers 76 33
Optimized Users 55 54
0
30
60
90
120
🟩 Yes
🟥 No

Over time Administrators add more and more group policies, as business requirements change. Due to neglection or thinking it may serve it's purpose later on a lot of Group Policies often have no value at all. Either the Group Policy is not linked to anything and just stays unlinked forever, or GPO is linked, but the link (links) are disabled or GPO is totally disabled. Then there are Group Policies that are targetting certain group or person and that group is removed leaving Group Policy doing nothing. Additionally sometimes new GPO is created without any settings or the settings are removed over time, but GPO stays in place.

- Group Policies total: **109**
- Group Policies valid: **22**
- Group Policies NOT valid: 87
  - Group Policies that are unlinked (are not doing anything currently): **88**
  - Group Policies that are empty (have no settings): **2**
  - Group Policies that are linked, but empty: **0**
  - Group Policies that are linked, but link disabled: **75**
  - Group Policies that are disabled (both user/computer sections): **0**
  - Group Policies that have no Apply Permission: **0**
- Group Policies NOT valid, to skip: 4 (modified less than 30 days ago)
- Group Policies recently modified: **7** (modified less than 30 days ago)

Following domains require actions (permissions required):

- james-rankin.com requires **87** changes.

Keep in mind that each GPO can match multiple conditions such as being empty and unlinked and disabled at the same time. We're only deleting GPO once.

All **empty** or **unlinked** or **disabled** Group Policies can be automatically deleted. Please review output in the table and follow steps below table to cleanup Group Policies. GPOs that have content, but are disabled require manual intervention. If performance is an issue you should consider disabling user or computer sections of GPO when those are not used.

Additionally, we're reviewing Group Policies that have their section disabled, but contain data.

- Group Policies with problems: **1**
  - Group Policies that have content (computer), but are disabled: **1**
  - Group Policies that have content (user), but are disabled: **0**

Such policies require manual review from whoever owns them. It could be a mistake tha section was disabled while containing data or that content is no longer needed in which case it should be deleted. This can't be auto-handled and is INFORMATIONAL only.

Following domains require actions (permissions required):

- james-rankin.com requires **1** changes.

Moreover, for best performance it's recommended that if there are no settings of certain kind (Computer or User settings) it's best to disable whole section.

- Group Policies with optimization:
  - Group Policies that are optimized (computer) **76**
  - Group Policies that are optimized (user): **55**
- Group Policies without optimization:
  - Group Policies that are not optimized (computer): **33**
  - Group Policies that are not optimized (user): **54**

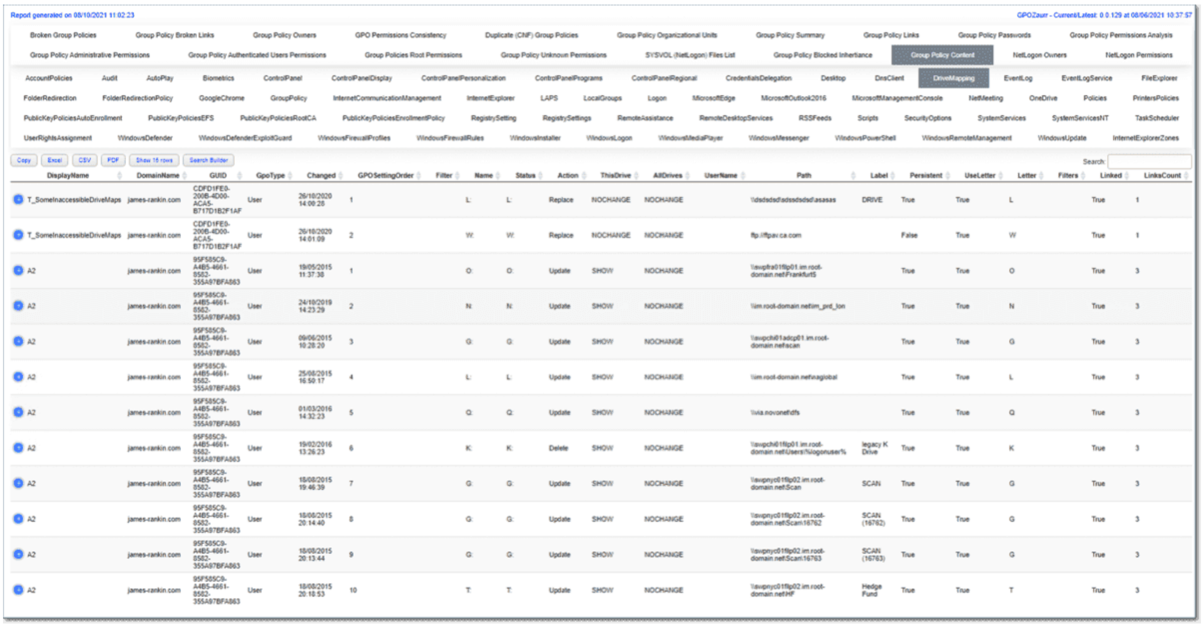
This means **85** could be optimized for performance reasons.

Following domains require actions (permissions required):

- james-rankin.com requires **85** changes.

GPOZaurr summary report

Another excellent feature of GPOZaurr is the ability to export any of the report sections to CSV (for manipulation in Excel), PDF, or HTML format. This allows you to pull out certain subsets of data and then produce more granular information. For instance, I have used it to look at data from the Group Policy Content section and then filter it by Drive Mappings to obtain a list of UNC paths that are being mapped via GP before exporting to CSV. This allowed me to identify any invalid or inaccessible drive mappings being delivered to the users.



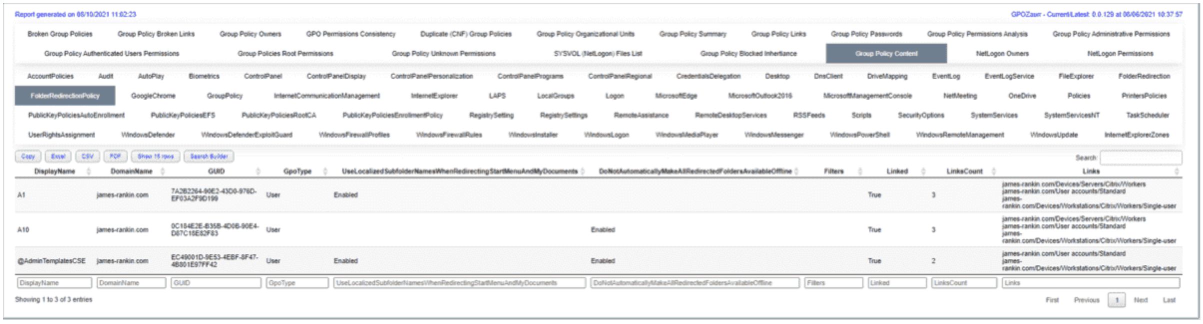
Report generated on 08/10/2021 11:02:23

GPOZaurr - Current/Latest: 0.0.129 at 08/06/2021 10:37:57

DisplayName	DomainName	GUID	GpoType	Changed	GPOSettingOrder	Filter	Name	Status	Action	ThisDrive	AllDrives	UserName	Path	Label	Persistent	UseLetter	Letter	Filters	Linked	LinksCount
T_SomeInaccessibleDriveMaps	james-rankin.com	CDFD1FE0-200B-4D00-ACA5-B717D1B2F1AF	User	26/10/2020 14:00:28	1		L:	L:	Replace	NOCHANGE	NOCHANGE		\\dsdsdsd\sdssdsdsd\asasas	DRIVE	True	True	L		True	1
T_SomeInaccessibleDriveMaps	james-rankin.com	CDFD1FE0-200B-4D00-ACA5-B717D1B2F1AF	User	26/10/2020 14:01:09	2		W:	W:	Replace	NOCHANGE	NOCHANGE		ftp://ftpav.ca.com		False	True	W		True	1
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	19/05/2015 11:37:38	1		O:	O:	Update	SHOW	NOCHANGE		\\awpfra01filp01.im.root-domain.net\Frankfurt5		True	True	O		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	24/10/2019 14:23:29	2		N:	N:	Update	SHOW	NOCHANGE		\\im.root-domain.net\im_prd_lon		True	True	N		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	09/06/2015 10:28:20	3		G:	G:	Update	SHOW	NOCHANGE		\\awpchi01adcp01.im.root-domain.net\scan		True	True	G		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	25/08/2015 16:50:17	4		L:	L:	Update	SHOW	NOCHANGE		\\im.root-domain.net\naglobal		True	True	L		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	01/03/2016 14:32:23	5		Q:	Q:	Update	SHOW	NOCHANGE		\\via.novonet\dfs		True	True	Q		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	19/02/2016 13:26:23	6		K:	K:	Delete	SHOW	NOCHANGE		\\awpchi01filp01.im.root-domain.net\Users\%logonuser%	legacy K Drive	True	True	K		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	18/08/2015 19:46:39	7		G:	G:	Update	SHOW	NOCHANGE		\\awpnyc01filp02.im.root-domain.net\Scan	SCAN	True	True	G		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	18/08/2015 20:14:40	8		G:	G:	Update	SHOW	NOCHANGE		\\awpnyc01filp02.im.root-domain.net\Scan\16762	SCAN (16762)	True	True	G		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	18/08/2015 20:13:44	9		G:	G:	Update	SHOW	NOCHANGE		\\awpnyc01filp02.im.root-domain.net\Scan\16763	SCAN (16763)	True	True	G		True	3
A2	james-rankin.com	95F585C9-A4B5-4661-8582-355A97BFA863	User	18/08/2015 20:18:53	10		T:	T:	Update	SHOW	NOCHANGE		\\awpnyc01filp02.im.root-domain.net\HF	Hedge Fund	True	True	T		True	3

GPOZaurr report filtered

Looking through the data available in this HTML file gives you fantastic insight into the setup and configuration of your Group Policies. There are some annoyances (such as spelling and grammatical mistakes) that can be chalked up to the author not having English as a first language, but you can easily tidy these up by editing the HTML directly. Of particular interest to me is the Group Policy Content section, which provides a wealth of data that can be perused or exported.



Report generated on 08/10/2021 11:02:23

GPOZaurr - Current/Latest: 0.0.129 at 08/06/2021 10:37:57

DisplayName	DomainName	GUID	GpoType	UseLocalizedSubfolderNamesWhenRedirectingStartMenuAndMyDocuments	DoNotAutomaticallyMakeAllRedirectedFoldersAvailableOffline	Filters	Linked	LinksCount	Links
A1	james-rankin.com	7A2B2264-90E2-43D0-976D-EF03A2F9D199	User	Enabled			True	3	james-rankin.com/Devices/Servers/Citrix/Workers james-rankin.com/User accounts/Standard james-rankin.com/Devices/Workstations/Citrix/Workers/Single-user
A10	james-rankin.com	0C184E2E-B35B-4D0B-90E4-D87C18E82F83	User		Enabled		True	3	james-rankin.com/Devices/Servers/Citrix/Workers james-rankin.com/User accounts/Standard james-rankin.com/Devices/Workstations/Citrix/Workers/Single-user
@AdminTemplatesCSE	james-rankin.com	EC49001D-9E53-4EBF-8F47-4B801E97FF42	User	Enabled	Enabled		True	2	james-rankin.com/User accounts/Standard james-rankin.com/Devices/Workstations/Citrix/Workers/Single-user
DisplayName	DomainName	GUID	GpoType	UseLocalizedSubfolderNamesWhenRedirectingStartMenuAndMyDocuments	DoNotAutomaticallyMakeAllRedirectedFoldersAvailableOffline	Filters	Linked	LinksCount	Links

Showing 1 to 3 of 3 entries

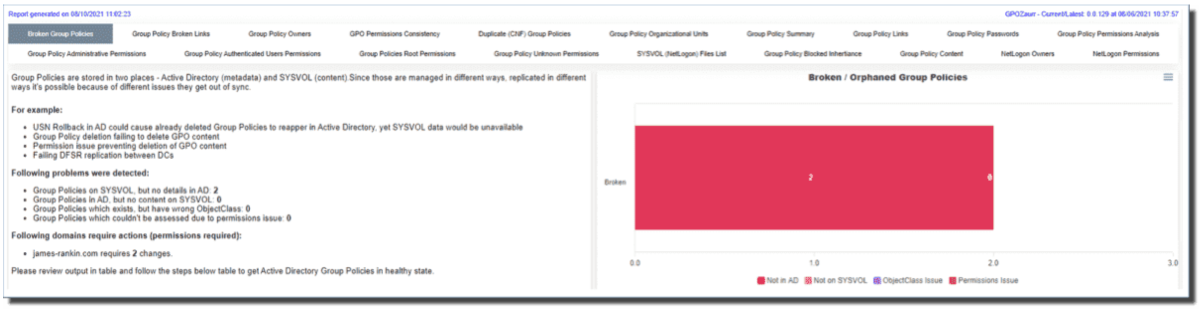
GPOZaurr content view

One cautionary mention is that GPOZaurr also provides links to remediation for things such as invalid GPOs or broken links. I would not recommend using this functionality—use the data that has been identified to feed into formal change controls for the removal of GPOs rather than using the tool to do them directly. As such, you should be careful who you provide the raw HTML data to—it is much safer to export the highlights to Excel or PDF for distribution purposes. If you want to avoid the remediation links and distribute HTML, however, you can simply run the tool with the *-HideSteps* parameter specified.

Some of the report sections that GPOZaurr outputs are immediately usable, whereas others require more detailed review. It is up to you how you use the data; you can filter and crunch it in any way you please. What I have suggested below is simply a list of guidelines. There are many more things you can achieve!

Finding broken GPOs

Broken or dead links are instantly identified.


Report generated on 08/10/2021 11:02:23
GPOZaurr - Current/Latest: 0.0.129 at 06/06/2021 10:37:57
Broken Group Policies
Group Policy Broken Links
Group Policy Owners
GPO Permissions Consistency
Duplicate (CNF) Group Policies
Group Policy Organizational Units
Group Policy Summary
Group Policy Links
Group Policy Passwords
Group Policy Permissions Analysis
Group Policy Administrative Permissions
Group Policy Authenticated Users Permissions
Group Policies Root Permissions
Group Policy Unknown Permissions
SYSVOL (NetLogon) Files List
Group Policy Blocked Inheritance
Group Policy Content
NetLogon Owners
NetLogon Permissions
Broken / Orphaned Group Policies
Broken
2
0
0.0
1.0
2.0
3.0
Not in AD
Not on SYSVOL
ObjectClass Issue
Permissions Issue

Group Policies are stored in two places - Active Directory (metadata) and SYSVOL (content).Since those are managed in different ways, replicated in different ways it's possible because of different issues they get out of sync.

For example:

- USN Rollback in AD could cause already deleted Group Policies to reapper in Active Directory, yet SYSVOL data would be unavailable
- Group Policy deletion failing to delete GPO content
- Permission issue preventing deletion of GPO content
- Failing DFSR replication between DCs

Following problems were detected:

- Group Policies on SYSVOL, but no details in AD: **2**
- Group Policies in AD, but no content on SYSVOL: **0**
- Group Policies which exists, but have wrong ObjectClass: **0**
- Group Policies which couldn't be assessed due to permissions issue: **0**

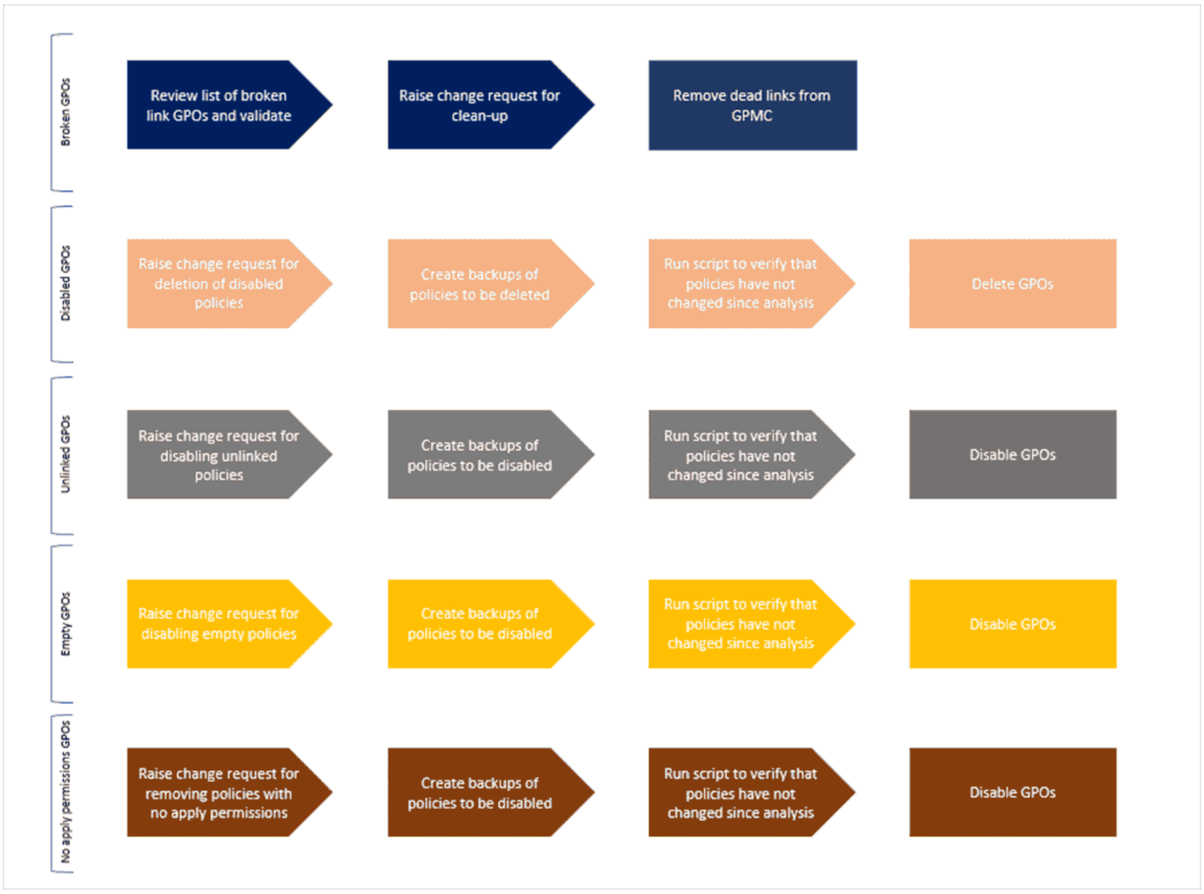
Following domains require actions (permissions required):

- james-rankin.com requires **2** changes.

Please review output in table and follow the steps below table to get Active Directory Group Policies in healthy state.

Finding broken GPOs links

The tool also pulls out GPOs that are disabled, duplicated, unlinked, empty, that have sections with disabled content, that users have no permissions to apply, and that have incorrect permissions. This gives a whole load of data that can be quickly verified and fed into a process to remove or disable policies that are not applied for a multitude of reasons. This should be properly validated and change reviewed, as shown in the process below. And it is always prudent to rerun the GPOZaurr utility before making any changes to make sure no one has altered the policies in the meantime.

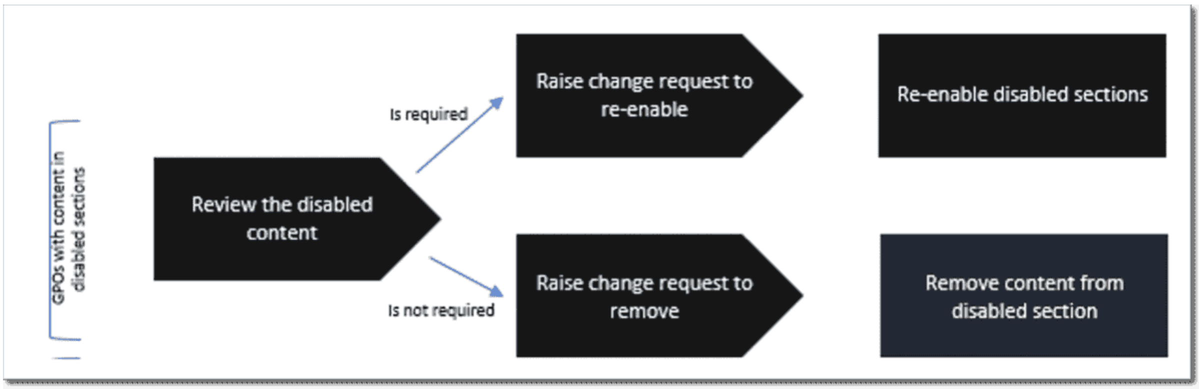

Broken GPOs
Review list of broken link GPOs and validate
Raise change request for clean-up
Remove dead links from GPMC
Disabled GPOs
Raise change request for deletion of disabled policies
Create backups of policies to be deleted
Run script to verify that policies have not changed since analysis
Delete GPOs
Unlinked GPOs
Raise change request for disabling unlinked policies
Create backups of policies to be disabled
Run script to verify that policies have not changed since analysis
Disable GPOs
Empty GPOs
Raise change request for disabling empty policies
Create backups of policies to be disabled
Run script to verify that policies have not changed since analysis
Disable GPOs
No apply permissions GPOs
Raise change request for removing policies with no apply permissions
Create backups of policies to be disabled
Run script to verify that policies have not changed since analysis
Disable GPOs

Fixing broken GPOs

In large enterprise environments, this stage of consolidation usually produces at least a few hundred policy objects that can potentially be removed. Once the "quick wins" are done, you can now move on to the slightly more time-consuming phases.

Finding disabled GPOs

First, there will be GPOs identified that have sections (either Computer or User Config) that are disabled but contain content. GPOZaurr will flag these, but they will need a manual review process to verify whether disabled content is required or not.

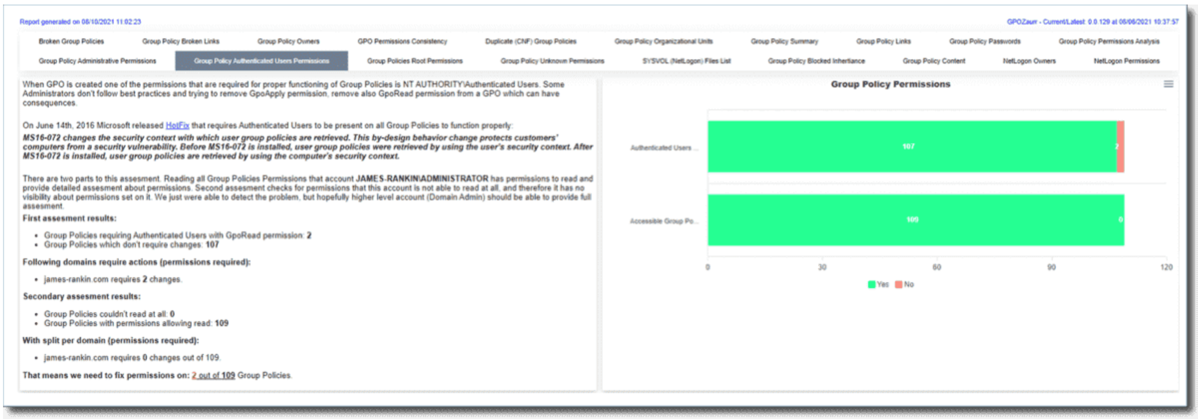

GPOs with content in disabled sections
Review the disabled content
Is required
Is not required
Raise change request to re-enable
Raise change request to remove
Re-enable disabled sections
Remove content from disabled section

Finding disabled GPOs

Finding GPOs with invalid security filters

Next is the specter of invalid security filters. Older GP implementations typically have more of these. Several years ago, Microsoft changed the way that the *user* Group Policy is applied via a security update. Some of the *user* processing is now done in the *device* context. This means that if you are filtering a GPO by user or group (and Authenticated Users is not present), then the Domain Computers group (or a list of computer accounts) must be present in order for the filter to successfully apply. GPOs that do not have Authenticated Users or a list of computer accounts specified on the Security Filter cannot be processed.

GPOZaurr outputs a report of "Group Policy Authenticated Users Permissions," which narrows the list down to policies that don't have Authenticated Users present, but each one of these must be checked manually for a group of computers being specified.


Report generated on 08/10/2021 11:02:23
GPOZaurr - Current/Latest: 0.0.129 at 08/06/2021 10:37:57
Broken Group Policies
Group Policy Broken Links
Group Policy Owners
GPO Permissions Consistency
Duplicate (CNF) Group Policies
Group Policy Organizational Units
Group Policy Summary
Group Policy Links
Group Policy Passwords
Group Policy Permissions Analysis
Group Policy Administrative Permissions
Group Policy Authenticated Users Permissions
Group Policies Root Permissions
Group Policy Unknown Permissions
SYSVOL (NetLogon) Files List
Group Policy Blocked Inheritance
Group Policy Content
NetLogon Owners
NetLogon Permissions
Group Policy Permissions
Authenticated Users ...
Accessible Group Po...
107
2
109
0
0
30
60
90
120
🟩 Yes 🟥 No

When GPO is created one of the permissions that are required for proper functioning of Group Policies is NT AUTHORITY\Authenticated Users. Some Administrators don't follow best practices and trying to remove GpoApply permission, remove also GpoRead permission from a GPO which can have consequences.

On June 14th, 2016 Microsoft released HotFix that requires Authenticated Users to be present on all Group Policies to function properly:

MS16-072 changes the security context with which user group policies are retrieved. This by-design behavior change protects customers' computers from a security vulnerability. Before MS16-072 is installed, user group policies were retrieved by using the user's security context. After MS16-072 is installed, user group policies are retrieved by using the computer's security context.

There are two parts to this assesment. Reading all Group Policies Permissions that account **JAMES-RANKIN\ADMINISTRATOR** has permissions to read and provide detailed assesment about permissions. Second assesment checks for permissions that this account is not able to read at all, and therefore it has no visibility about permissions set on it. We just were able to detect the problem, but hopefully higher level account (Domain Admin) should be able to provide full assesment.

First assesment results:

- Group Policies requiring Authenticated Users with GpoRead permission: **2**
- Group Policies which don't require changes: **107**

Following domains require actions (permissions required):

- james-rankin.com requires **2** changes.

Secondary assesment results:

- Group Policies couldn't read at all: **0**
- Group Policies with permissions allowing read: **109**

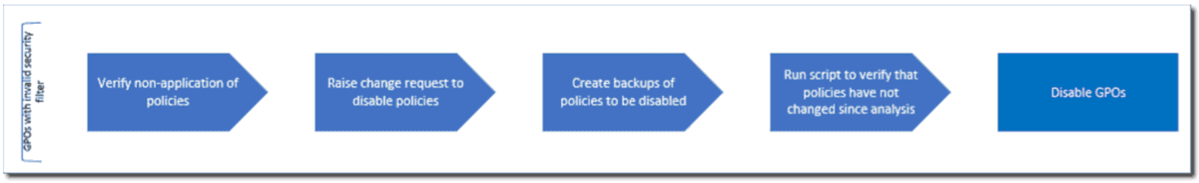
With split per domain (permissions required):

- james-rankin.com requires **0** changes out of 109.

That means we need to fix permissions on: 2 out of 109 Group Policies.

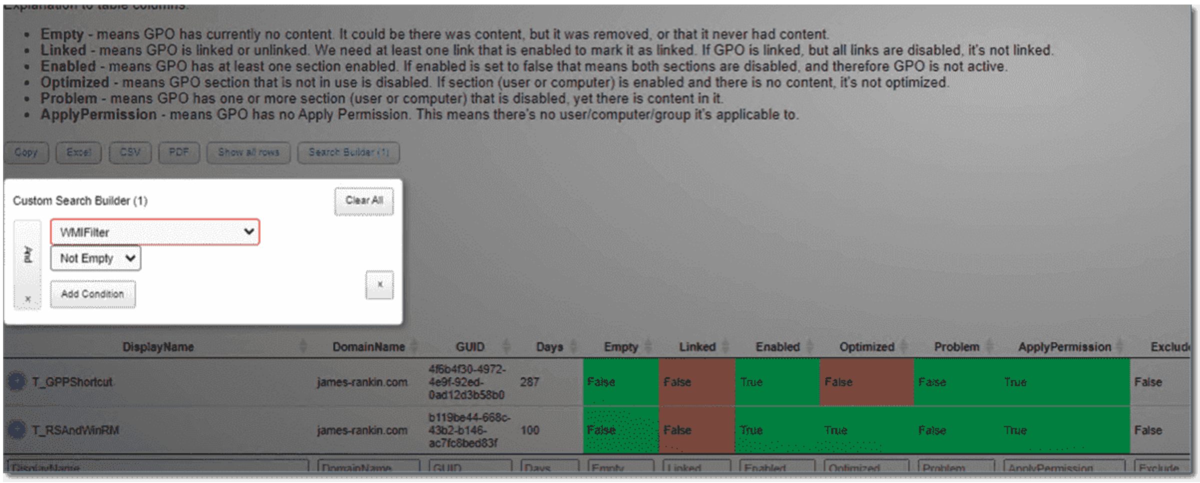
GPOs with invalid security filters

If there are no computer groups or accounts present on the Security Filter, however, this indicates that the GPO has an invalid security filter and should be either remediated or removed.


GPOs with invalid security filter
Verify non-application of policies
Raise change request to disable policies
Create backups of policies to be disabled
Run script to verify that policies have not changed since analysis
Disable GPOs

Fixing GPOs with invalid security filter

You can also apply custom Search Builder conditions to the GPOZaurr data to produce more targeted inquiries. I used this to filter the summary data down into those policies containing WMI filters. It is useful to view and verify these to ensure that they are still applicable and don't take a long time to apply (Product Class is a well-known WMI filter that will cause particular issues).



- **Empty** - means GPO has currently no content. It could be there was content, but it was removed, or that it never had content.
- **Linked** - means GPO is linked or unlinked. We need at least one link that is enabled to mark it as linked. If GPO is linked, but all links are disabled, it's not linked.
- **Enabled** - means GPO has at least one section enabled. If enabled is set to false that means both sections are disabled, and therefore GPO is not active.
- **Optimized** - means GPO section that is not in use is disabled. If section (user or computer) is enabled and there is no content, it's not optimized.
- **Problem** - means GPO has one or more section (user or computer) that is disabled, yet there is content in it.
- **ApplyPermission** - means GPO has no Apply Permission. This means there's no user/computer/group it's applicable to.

Custom Search Builder (1)

WMIFilter

Not Empty

DisplayName	DomainName	GUID	Days	Empty	Linked	Enabled	Optimized	Problem	ApplyPermission	Exclud
T_GPPShortcut	james-rankin.com	4f6b4f30-4972-4e9f-92ed-0ad12d3b58b0	287	False	False	True	False	False	True	False
T_RSAndWinRM	james-rankin.com	b119be44-668c-43b2-b146-ac7fc8bed83f	100	False	False	True	True	False	True	False

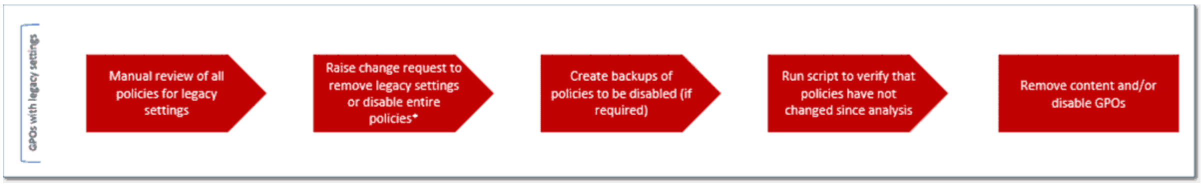
Custom search builder

Finding inapplicable GPOs

For the final part of the medium-term remediation, you can assess whether GPO settings are inapplicable. Many GPOs, for instance, apply only to particular operating systems or software versions (such as settings that only apply to Windows XP and Server 2003). These settings, if present, will still be applied (they are just registry entries), but are essentially ignored. Therefore, it is useful to identify and remediate these.

This is one area where, surprisingly, GPOZaurr does not offer much. However, Microsoft also has the Policy Analyzer tool available, which may help with this in enterprise environments. This tool compares GPOs to look for invalid settings.

Once you have identified any invalid legacy policies (whether by using Policy Analyzer or by manual review), you can then feed the policies into the usual change review process to get them removed.


GPOs with legacy settings
Manual review of all policies for legacy settings
Raise change request to remove legacy settings or disable entire policies*
Create backups of policies to be disabled (if required)
Run script to verify that policies have not changed since analysis
Remove content and/or disable GPOs

Fixing inapplicable GPOs

In my next post, I will cover Loopback Policy Processing, Folder Redirection, and your monthly Group Policy clean-up tasks.