

# The only command you will ever need to understand and fix your Group Policies (GPO)

[evotec.xyz/the-only-command-you-will-ever-need-to-understand-and-fix-your-group-policies-gpo/](https://evotec.xyz/the-only-command-you-will-ever-need-to-understand-and-fix-your-group-policies-gpo/)

January 24, 2021

• ad.evotec.xyz requires 0 changes.  
Following domains require fixing using different methods:  
• ad.evotec.pl requires 3 changes.  
• ad.evotec.xyz requires 1 changes.

Display Name	Domain Name	GUID	Owner	Owner SID	Owner Type	Sysvol Owner	Sysvol SID	Sysvol Type	Sysvol Path	Is Owner Consistent	Is Owner Administrative	Sysvol Exists	Distinguished Name
New Group Policy Object3	ad.evotec.xyz	98A5284F-4ABF-46A7-802F-84FC026E9444	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative			Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{98A5284F-4ABF-46A7-802F-84FC026E9444}	False	False	False	CN=98A5284F-4ABF-46A7-802F-84FC026E9444,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz
DC: PowerShell Logging	ad.evotec.pl	7112AF81-5CB7-4010-808D-C0F11FAFD714	EVOTEC\Domain Admins	0-5-521-366118273-382079955-297026695-512	Administrative			Administrative	\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{7112AF81-5CB7-4010-808D-C0F11FAFD714}	False	False	False	CN=7112AF81-5CB7-4010-808D-C0F11FAFD714,CN=Polices,CN=System,DC=ad,DC=evotec,DC=pl
DC: Configure Time PDC	ad.evotec.pl	24194523-8882-439C-A533-ABF4F3FA2C24	EVOTEC\Domain Admins	0-5-521-366118273-382079955-297026695-512	Administrative			Administrative	\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{24194523-8882-439C-A533-ABF4F3FA2C24}	False	False	False	CN=24194523-8882-439C-A533-ABF4F3FA2C24,CN=Polices,CN=System,DC=ad,DC=evotec,DC=pl
TEST Empty GPO - ad.evotec.pl, CrossDomain GPO	ad.evotec.pl	EAD2884-113F-4102-977B-D5D1212F4F91	EVOTEC\Enterprise Admins	0-5-521-853615985-2870443239-316398659-519	Administrative			Administrative	\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{EAD2884-113F-4102-977B-D5D1212F4F91}	False	False	False	CN=EAD2884-113F-4102-977B-D5D1212F4F91,CN=Polices,CN=System,DC=ad,DC=evotec,DC=pl
Default Domain Policy	ad.evotec.pl	3182734D-016D-1102-949F-00C4F8984F9	EVOTEC\Domain Admins	0-5-521-366118273-382079955-297026695-512	Administrative	BUILTIN\Administrators	0-5-5-52-544	WellKnownAdministrative	\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{3182734D-016D-1102-949F-00C4F8984F9}	False	False	True	CN=3182734D-016D-1102-949F-00C4F8984F9,CN=Polices,CN=System,DC=ad,DC=evotec,DC=pl
Default Domain Controllers Policy	ad.evotec.pl	6AC1786C-016F-1102-949F-00C4F8984F9	EVOTEC\Domain Admins	0-5-521-366118273-382079955-297026695-512	Administrative	BUILTIN\Administrators	0-5-5-52-544	WellKnownAdministrative	\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{6AC1786C-016F-1102-949F-00C4F8984F9}	False	False	True	CN=6AC1786C-016F-1102-949F-00C4F8984F9,CN=Polices,CN=System,DC=ad,DC=evotec,DC=pl
Default Domain Policy	ad.evotec.xyz	3182734D-016D-1102-949F-00C4F8984F9	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{3182734D-016D-1102-949F-00C4F8984F9}	True	True	True	CN=3182734D-016D-1102-949F-00C4F8984F9,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz
Default Domain Controllers Policy	ad.evotec.xyz	6AC1786C-016F-1102-949F-00C4F8984F9	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{6AC1786C-016F-1102-949F-00C4F8984F9}	True	True	True	CN=6AC1786C-016F-1102-949F-00C4F8984F9,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz
DC: Event Log Settings	ad.evotec.xyz	4E1FC7D-10DB-4A86-8BA3-14A8E07F0848	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{4E1FC7D-10DB-4A86-8BA3-14A8E07F0848}	True	True	True	CN=4E1FC7D-10DB-4A86-8BA3-14A8E07F0848,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz
DC: Event Log Audit Rules	ad.evotec.xyz	59F83860-74C9-4262-A077-80167F820000	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative	EVOTEC\Domain Admins	0-5-521-853615985-2870443239-316398659-512	Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{59F83860-74C9-4262-A077-80167F820000}	True	True	True	CN=59F83860-74C9-4262-A077-80167F820000,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz

I've been working on cleaning up **Group Policies** for a couple of months. While it may seem trivial, things get complicated when you're tasked with managing 5000 **GPOs** created over 15 years by multiple teams without any best practices in mind. While working on **GPOZaurr** (my new **PowerShell** module), I've noticed that the more code I wrote to manage those **GPOs**, the more I knew passing this knowledge to admins who will be executing this on a **weekly/monthly basis** is going to be a challenge. That's why I've decided to follow a similar approach as my other Active Directory testing module called **Testimo**. I've created a single command that analyses **Group Policies** using different methods and shows views from different angles to deliver the full picture. On top of that, it provides a solution (or it tries to) so that it's fairly easy to fix – as long as you agree with what it proposes.

Please be careful when using this on production

I've done a lot of research and put a lot of effort into making sure this **PowerShell** module works as expected. However, I do make mistakes. Contrary to my usual work, this module is not read-only. To almost every read command, there is also a set or remove command. It can change things, delete them, or modify them. If you don't understand what will happen, don't do it. Review source code, run read commands first to understand the output, what it's showing. If you have doubts – don't use it or create an issue on **GitHub** to clarify. All cmdlets that have the ability to write/delete contain **WhatIf/LimitProcessing** count parameters. Use them before implementing any changes!

**Please keep in mind I've tested GPOZaurr only on English based Active Directory.** I have no clue how it will behave on non-English systems. As I've not worked with other languages for a while, I don't remember if object types are still reported in English by PowerShell or reported in language equivalent. Be careful.

### *Useful Links*

Please make sure to visit **GitHub** to review sources or report issues. If you're going to use it, I recommend doing it via **PowerShellGallery** as that version is minimized and optimized. Reviewing sources is easier on the GitHub version as it has more comments and is divided into sections.

The code is published on [GitHub](#)

Issues should be reported on [GitHub](#)

Code is published as a module on [PowerShellGallery](#).

The module is signed with a certificate, like any new modules that I create or update.

```
Install-Module GPOZaurr -Force
```

### *Invoke-GPOZaurr - One command that makes a difference*

As mentioned before, **Invoke-GPOZaurr** follows a similar pattern to what **Invoke-Testimo** does. When run without any parameters, it will go thru all available reports one by one to deliver a full-scope scan. Keep in mind that running this cmdlet without any parameters is fine for small domains, but it will take hours to complete for larger domains. For the domain of 5000 GPOs, some reports can take even 2 hours to complete.

```
PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\przemyslaw.kly> Invoke-GPOZaurr
[i][GPOZaurr] Version [Informative] Current/Latest: 0.0.110 at 01/22/2021 12:41:11
[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, 780 milliseconds]
[i][Start] Group Policy Broken Links
[i][End ] Group Policy Broken Links [Time to execute: 0 days, 0 hours, 0 minutes, 1 seconds, 101 milliseconds]
[i][Start] Group Policy Owners
[i][End ] Group Policy Owners [Time to execute: 0 days, 0 hours, 0 minutes, 2 seconds, 989 milliseconds]
[i][Start] GPO Permissions Consistency
WARNING: Get-GPOZaurrPermissionConsistency - Processing New Group Policy Object3 / ad.evotec.xyz failed as path
\\ad.evotec.xyz\sysvol\ad.evotec.xyz\Policies\{59a50b4f-9abf-46a7-802f-84fc0d6ef944} doesn't exists!
WARNING: Get-GPOZaurrPermissionConsistency - Processing DC | Configure Time PDC / ad.evotec.pl failed as path
\\ad.evotec.pl\sysvol\ad.evotec.pl\Policies\{24194523-bb82-439c-a533-abf4f30fa2c4} doesn't exists!
WARNING: Get-GPOZaurrPermissionConsistency - Processing DC | PowerShell Logging / ad.evotec.pl failed as path
\\ad.evotec.pl\sysvol\ad.evotec.pl\Policies\{7112af81-5cb7-401c-8d8d-c0f11fafd714} doesn't exists!
WARNING: Get-GPOZaurrPermissionConsistency - Processing TEST | Empty GPO - AD.EVOTEC.PL CrossDomain GPO / ad.evotec.pl
failed as path \\ad.evotec.pl\sysvol\ad.evotec.pl\Policies\{eade3894-113f-4100-977b-d5d121df4f91} doesn't exists!
[i][End ] GPO Permissions Consistency [Time to execute: 0 days, 0 hours, 0 minutes, 9 seconds, 754 milliseconds]
[i][Start] Duplicate (CNF) Group Policies
[i][End ] Duplicate (CNF) Group Policies [Time to execute: 0 days, 0 hours, 0 minutes, 0 seconds, 530 milliseconds]
[i][Start] Group Policy Summary
WARNING: Get-PrivGPOZaurrLink - Couldn't find link ad.evotec.xyz8A7BC515-D7FD-4D1F-90B8-E47C15F89295 in a GPO Cache.
Lack of permissions for given GPO? Are you running as admin? Skipping.
[i][End ] Group Policy Summary [Time to execute: 0 days, 0 hours, 0 minutes, 14 seconds, 293 milliseconds]
[i][Start] Group Policy Links
WARNING: Get-PrivGPOZaurrLink - Couldn't find link ad.evotec.xyz8A7BC515-D7FD-4D1F-90B8-E47C15F89295 in a GPO Cache.
Lack of permissions for given GPO? Are you running as admin? Skipping.
[i][End ] Group Policy Links [Time to execute: 0 days, 0 hours, 0 minutes, 0 seconds, 707 milliseconds]
[i][Start] Group Policy Passwords
WARNING: Get-GPOZaurrPassword - Access to the path
'\\ad.evotec.xyz\sysvol\ad.evotec.xyz\Policies\{8A7BC515-D7FD-4D1F-90B8-E47C15F89295}' is denied.
(UnauthorizedAccessException)
[i][End ] Group Policy Passwords [Time to execute: 0 days, 0 hours, 0 minutes, 1 seconds, 703 milliseconds]
[i][Start] Group Policy Permissions Analysis
[i][End ] Group Policy Permissions Analysis [Time to execute: 0 days, 0 hours, 0 minutes, 3 seconds, 270 milliseconds]
```

When run, it will display a short information about what it is currently doing and which report is being generated. If you have a large domain and things take time, you may want to use **Invoke-GPOZaurr** with **Verbose** parameter to get additional information.

```
PowerShell x Windows PowerShell x + v
PS C:\Users\przemyslaw.klys> Invoke-GPOZaurr -Verbose
[i][GPOZaurr] Version [Informative] Current/Latest: 0.0.110 at 01/22/2021 12:41:11
[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
VERBOSE: Get-GPOZaurrBroken - Starting process for ad.evotec.xyz
VERBOSE: Get-GPOZaurrBroken - Processing SYSVOL from \\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](1/47) TEST | Registry GPOs
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](2/47) ALL | Enable RDP
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](3/47) COMPUTERS | Add Administrator
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](4/47) TEST | Password Filter
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](5/47) TEST | Local Users and Groups
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](6/47) ALL | Allow use of biometrics
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](7/47) TEST | BitLocker Settings
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](8/47) TEST | GPOZaurr Permissions Testing
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](9/47) TEST | Empty GPO Block Admin
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](10/47) New Group Policy Object
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](11/47) TEST | Event Log Audit Rules
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](12/47) ALL | Certificates
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](13/47) Default Domain Policy
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](14/47) TEST | Container 2
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](15/47) ALL | Trusted Websites
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](16/47) Copy of ALL | Trusted Websites
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](17/47) ALL | BitLocker Settings
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](18/47) DC | Event Log Settings
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](19/47) DC | Event Log Audit Rules
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](20/47) New Group Policy Object3
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](21/47) ALL | Firewall Settings
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](22/47) COMPUTERS | Enable Sets
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](23/47) TEST | IE Testing
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](24/47) TEST | Drive Mapping
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](25/47) Default Domain Controllers Policy
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](26/47) TEST | Container 1
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](27/47) TEST | LAPS
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](28/47) TEST | Task
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](29/47) DC | Password Filter
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](30/47) ALL | Windows PowerShell
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](31/47) {8A7BC515-D7FD-4D1F-90B8-E47C15F89295}
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](32/47) TEST | Task Schedule 1
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](33/47) COMPUTERS | LAPS
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](34/47) TEST | Deny Admins
VERBOSE: Get-GPOZaurrBroken - Processing [ad.evotec.xyz](35/47) TEST | CrossLink To AD.EVOTEC.PL
```

Once the cmdlet is complete HTML report will open up automatically.

Broken Group Policies

Group Policy Broken Links    Group Policy Owners    GPO Permissions Consistency    Duplicate (CNF) Group Policies    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 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 reappear 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: 4
- Group Policies which exists, but have wrong ObjectClass: 0
- Group Policies which couldn't be added due to permissions issue: 1

**Following domains require actions (permissions required):**

- ad.evotec.pl requires 3 changes.
- ad.evotec.yz requires 3 changes.

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

**Broken / Orphaned Group Policies**

■ Not in AD   
 ■ Not on SYSVOL   
 ■ ObjectClass Issue   
 ■ Permissions Issue

**Health State of Group Policies**

Copy    Excel    CSV    PDF    Show 10 rows

DisplayName	Status	DomainName	SysvolServer	ObjectClass	Id	Path	DistinguishedName	Description	CreationTime	ModificationTime	Error
{280B0713-760D-4957-809F-672160A276E9}	Not available in AD	ad.evotec.yz	ad.evotec.yz		{280B0713-760D-4957-809F-672160A276E9}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{280B0713-760D-4957-809F-672160A276E9}	CN={280B0713-760D-4957-809F-672160A276E9},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2020-10-19 10:00:20	2020-10-19 10:00:20	
{8A78C515-57FB-4D1F-908B-E47C15F89295}	Permissions issue	ad.evotec.yz	ad.evotec.yz		{8A78C515-57FB-4D1F-908B-E47C15F89295}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{8A78C515-57FB-4D1F-908B-E47C15F89295}	CN={8A78C515-57FB-4D1F-908B-E47C15F89295},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz				
{C0A8B503-121B-4896-8E52-C5E371896A17}	Not available in AD	ad.evotec.yz	ad.evotec.yz		{C0A8B503-121B-4896-8E52-C5E371896A17}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{C0A8B503-121B-4896-8E52-C5E371896A17}	CN={C0A8B503-121B-4896-8E52-C5E371896A17},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2020-10-19 10:00:34	2020-10-19 10:00:34	
ALL   Allow use of biometrics	Exists	ad.evotec.yz	ad.evotec.yz	groupPolicyContainer	{110F0E76E-D985-4FA4-91A4-C2F7830827AA}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{110F0E76E-D985-4FA4-91A4-C2F7830827AA}	CN={110F0E76E-D985-4FA4-91A4-C2F7830827AA},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2018-05-20 23:50:07	2020-11-26 10:24:11	
ALL   Bitlocker Settings	Exists	ad.evotec.yz	ad.evotec.yz	groupPolicyContainer	{3E07E1A0-357F-4638-88F0-F2E8404E74E5}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{3E07E1A0-357F-4638-88F0-F2E8404E74E5}	CN={3E07E1A0-357F-4638-88F0-F2E8404E74E5},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2018-08-07 12:22:23	2020-05-19 20:24:10	
ALL   Certificates	Exists	ad.evotec.yz	ad.evotec.yz	groupPolicyContainer	{2C7652B8-C1A1-42C1-8B46-D620A70E9356}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{2C7652B8-C1A1-42C1-8B46-D620A70E9356}	CN={2C7652B8-C1A1-42C1-8B46-D620A70E9356},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2020-06-06 20:03:36	2020-06-17 08:32:32	
ALL   Enable RDP	Exists	ad.evotec.yz	ad.evotec.yz	groupPolicyContainer	{0518C0DF-CC11-4278-B0F0-684C0A6E3D08}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{0518C0DF-CC11-4278-B0F0-684C0A6E3D08}	CN={0518C0DF-CC11-4278-B0F0-684C0A6E3D08},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2018-08-07 12:47:44	2020-12-06 10:19:36	
ALL   Firewall Settings	Exists	ad.evotec.yz	ad.evotec.yz	groupPolicyContainer	{617E6E45-16D6-4330-8D09-60E14B3047}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{617E6E45-16D6-4330-8D09-60E14B3047}	CN={617E6E45-16D6-4330-8D09-60E14B3047},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2018-08-07 16:42:25	2020-11-11 13:29:04	
ALL   Trusted Websites	Exists	ad.evotec.yz	ad.evotec.yz	groupPolicyContainer	{370C53AA-5298-4C0D-8977-3F3778269FC8}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{370C53AA-5298-4C0D-8977-3F3778269FC8}	CN={370C53AA-5298-4C0D-8977-3F3778269FC8},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2020-05-09 10:03:32	2020-05-09 10:16:43	
ALL   Windows PowerShell	Exists	ad.evotec.yz	ad.evotec.yz	groupPolicyContainer	{810F1158-2225-4919-AC72-08607917D070}	\\ad.evotec.yz\SYSVOL\ad.evotec.yz\Policies\{810F1158-2225-4919-AC72-08607917D070}	CN={810F1158-2225-4919-AC72-08607917D070},CN=Policies,CN=System,DC=ad,DC=evotec,DC=yz		2020-08-27 11:48:19	2020-08-27 11:49:44	

Showing 1 to 10 of 54 entries

**Steps to fix - Not available on SYSVOL / Active Directory / ObjectClass issue**

Prepare environment    Prepare report    Make a backup (optional)    Fix GPOs not available in AD    Fix GPOs not available on SYSVOL    Fix GPOs of wrong ObjectClass    Verification report

To be able to execute actions in automated way please install required modules. Those modules will be installed straight from Microsoft PowerShell Gallery.

- Install-Module GPOZaurr -Force
- Import-Module GPOZaurr -Force

Using force makes sure newest version is downloaded from PowerShellGallery regardless of what is currently installed. Once installed you're ready for next step.

Previous    Next

As you can see on the screenshot above, multiple reports were created, each on a different tab. The design of the report is mostly the same. There is information about what the report detected and why it did so on the report's top left. It also gives you a summary of your whole forest and where the issues are found. In the top right corner, I've added a small chart that visualizes the current status. Some charts will show only problems. Some will show multiple statuses – all depending on the type of report getting generated. There is usually one, but sometimes more tables with displayed information depending on the problem in the second section. Tables are color-coded to visualize better what is bad or to distinguish multiple problems within the same report. Tables also allow you to export data to Excel, CSV or PDF.

- ad.evotec.pl requires 3 changes.
- ad.evotec.xyz requires 44 changes.

To generate up to date report please execute:

- Install-Module GPOZaurr -Force or install module manually.
- Invoke-GPOZaurr -FilePath \$env:UserProfile\Desktop\GPOZaurr\GPOListBefore.html -Verbose -Type GPOList

Steps above will generate above summary with more details allowing you to get up to date report and steps on how to fix it.

Group Policies List

Explanation to table columns:

- **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.

Copy Excel CSV PDF Show 10 rows

Display Name	Domain Name	GUID	Days	Empty	Linked	Enabled	Optimized	Problem	Apply Permission	Exclude	Computer Policies	User Policies	Links Count	Links Enabled Count	Links Disabled Count	Enabled Details	Computer Problem	Computer Optimized
TEST   Registry GPOs	ad.evotec.xyz	01444204-02b5-4c9a-e539-660f42729c	76	False	False	False	False	True	True	False	Windows Registry		0	0	0	All settings disabled	True	False
ALL   Enable RDP	ad.evotec.xyz	0519c0df-c111-427b-b20f-63463a643dbb	48	False	True	True	False	False	True	False	Registry		7	6	1	Enabled	False	True
COMPUTERS   Add Administrator	ad.evotec.xyz	08794f6c-c541-429f-809c-09d83133910	211	False	False	False	False	False	True	False	Local Users and Groups		0	0	0	Enabled	False	True
TEST   Password Filter	ad.evotec.xyz	06d33b13-3477-4bc5-8c3e-38d93668343e	175	False	False	True	False	False	True	False	Registry		0	0	0	Enabled	False	True
TEST   Local Users and Groups	ad.evotec.xyz	10466a97-c7d2-485a-824b-9f45847702b6	76	False	False	True	False	True	True	False	Local Users and Groups, Local Users and Groups		0	0	0	User configuration settings disabled	False	True
ALL   Allow use of biometrics	ad.evotec.xyz	10f0e75e-d905-4f4a-9144-c27830827aa	58	False	True	True	True	False	True	False	Name Resolution Policy, Registry		4	3	1	User configuration settings disabled	False	True
TEST   Bitlocker Settings	ad.evotec.xyz	159efc16-c8f9-43b6-e179-57312a2b4355	175	False	False	True	False	False	True	False	Registry		0	0	0	Enabled	False	True
TEST   GPOZaurr Permissions Testing	ad.evotec.xyz	19effae7-8b10-4854-6099-446fd0de858	31	False	True	True	False	False	True	False	Registry		1	1	0	Enabled	False	False
TEST   Empty GPO Block Admin	ad.evotec.xyz	1be89b66-33fa-4b07-e68b-b4414b9c8066	192	True	False	True	False	False	True	False			0	0	0	Enabled	False	False
New Group Policy Object	ad.evotec.xyz	1d011660-6449-4151-b87e-e24487032776	73	True	False	True	False	False	False	False			0	0	0	Enabled	False	False

Showing 1 to 10 of 51 entries

Steps to fix - Empty & Unlinked & Disabled Group Policies

Following steps will guide you how to remove empty or unlinked group policies

Prepare environment → Prepare report → Make a backup → Excluding Group Policies → Remove GPOs that are EMPTY → Remove GPOs that are UNLINKED → Remove GPOs that are DISABLED → Remove GPOs that do not APPLY → Optimize GPOs (optional) → Verification report

To be able to execute actions in automated way please install required modules. Those modules will be installed straight from Microsoft PowerShell Gallery.

1. Install-Module GPOZaurr -Force
2. Import-Module GPOZaurr -Force

Using force makes sure newest version is downloaded from PowerShellGallery regardless of what is currently installed. Once installed you're ready for next step.

Previous Next

Finally, the last section contains the solution to the problem described. It usually provides step by step instructions on fixing the problem if you choose to fix it. Most of the time, solutions are automated to the point where a single line of code can fix an issue. For example, **delete all empty GPOs**, **delete all unlinked GPOs**, and so on. One command, zero effort.

### Invoke-GPOZaurr - Available reports

Currently, **Invoke-GPOZaurr** has few built-in reports. Some of them are more advanced, some of them are for review only. Here's the full list for today. Not everything is 100% finished. Some will require some updates soon as I get more time and feedback. Feel free to report issues/improve those reports with more information.

- **GPOBroken** – this report can detect GPOs that are broken. By broken GPOs, I mean those which exist in AD but have no SYSVOL content or vice versa – have SYSVOL content, but there's no AD metadata. Additionally, it's able to detect GPO objects that are no longer GroupPolicy object. – Then, it provides an easy way to fix it using given step-by-step instructions.
- **GPOBrokenLink** – this report can detect links that have no matching GPO. For example, if a GPO is deleted, sometimes links to that GPO are not properly removed. This command can detect that and propose a solution.



- **GPOOwners** – this report focuses on GPO Owners. By design, if Domain Admin creates GPO, the owner of GPO is the domain admins group. This report detects GPOs that are not owned by Domain Admins (in both SYSVOL and AD) and provides a way to fix them.
- **GPOConsistency** – this report detects inconsistent permissions between Active Directory and SYSVOL, verifying that files/folders inside each GPO match permissions as required. It then provides you an option to fix it.
- **GPODuplicates** – this report detects GPOs that are CNF, otherwise known as duplicate AD Objects, and provides a way to remove them.
- **GPOList** – this report summarizes all group policies focusing on detecting Empty, Unlinked, Disabled, No Apply Permissions GPOs. It also can detect GPOs that are not optimized or have potential problems (disabled section, but still settings in it)
- **GPOLinks** – this report summarizes links showing where the GPO is linked, whether it's linked to any site, cross-domain, or the status of links.
- **GPOPassword** – this report should detect passwords stored in GPOs.
- **GPOPermissions** – this report provides full permissions overview for all GPOs. It detects GPOs missing read permissions for Authenticated Users, GPOs that miss Domain Admins, Enterprise Admins, or SYSTEM permissions. It also detects GPOs that have Unknown permissions available. Finally, it allows you to fix permissions for all those GPOs easily. It's basically a one-stop for all permission needs.
- **GPOPermissionsAdministrative** – this report focuses only on detecting missing Domain Admins, Enterprise Admins permissions and allows you to fix those in no time.
- **GPOPermissionsRead** – similar to an administrative report, but this one focuses on Authenticated Users missing their permissions.
- **GPOPermissionsRoot** – this report shows all permissions assigned to the root of the group policy container. It allows you to verify who can manage all GPOs quickly.
- **GPOPermissionsUnknown** – this report focuses on detecting unknown permissions (deleted users) and allows you to remove them painlessly.
- **GPOFiles** – this report lists all files in the SYSVOL folder (including hidden ones) and tries to make a decent guess whether the file placement based on extension/type makes sense or requires additional verification. This was written to find potential malware or legacy files that can be safely deleted.
- **GPOBlockedInheritance** – this report checks for all Organizational Units with blocked inheritance and verifies the number of users or computers affected.
- **GPOAnalysis** – this report reads all content of group policies and puts them into 70+ categories. It can show things like GPOs that do Drive Mapping, Bitlocker, Laps, Printers, etc. It's handy to find dead settings, dead hosts, or settings that no longer make sense.
- **NetLogonOwners** – this report focuses on detecting NetLogon Owners and a way to fix it to default, secure values.
- **NetLogonPermissions** – this report provides an overview and assessment of all permissions on the NetLogon share.

## • SysVolLegacyFiles – this report detects SYSVOL Legacy Files (.adm) files

### Invoke-GPOZaurr - Report GPOBroken

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, and they get out of sync.

### Invoke-GPOZaurr -Type GPOBroken

Report generated on 01/23/2021 18:09:37 GPOZaurr - Current/Lastest: 0.0.110 at 01/22/2021 12:41:11

Broken Group Policies | Group Policy Broken Links | Group Policy Owners | GPO Permissions Consistency | Duplicate (CNF) Group Policies | 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) File List | Group Policy Blocked Inheritance | Group Policy Content | NetLogon Owners | NetLogon Permissions

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 reappear in Active Directory, yet SYSVOL data would be unavailable
- Group Policy deletion failing to delete GPO content
- Permission issue preventing deletion of GPO content
- Falling 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: 4
- Group Policies which exists, but have wrong ObjectClass: 0
- Group Policies which couldn't be assessed due to permissions issue: 1

**Following domains require actions (permissions required):**

- ad.evotec.pl requires 3 changes.
- ad.evotec.xyz requires 3 changes.

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

**Broken / Orphaned Group Policies**

Broken

■ Not in AD ■ Not on SYSVOL ■ ObjectClass Issue ■ Permissions Issue

Display Name	Status	Domain Name	Sysvol Server	Object Class	Id	Path	Distinguished Name	Description	Creation Time	Modification Time	Error
{280B0713-7650-4957-899F-672762479E9}	Not available in AD	ad.evotec.xyz	ad.evotec.xyz		{280B0713-7650-4957-899F-672762479E9}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{280B0713-7650-4957-899F-672762479E9}	CN={280B0713-7650-4957-899F-672762479E9},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2020-10-19 10:00:29	2020-10-19 10:00:29	
{8A78C515-07FD-4D1F-90B8-E47C15F89295}	Permissions issue	ad.evotec.xyz	ad.evotec.xyz		{8A78C515-07FD-4D1F-90B8-E47C15F89295}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{8A78C515-07FD-4D1F-90B8-E47C15F89295}	CN={8A78C515-07FD-4D1F-90B8-E47C15F89295},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2020-10-19 10:00:34	2020-10-19 10:00:34	
{CDAB8503-1218-4896-BE52-C5E371896A17}	Not available in AD	ad.evotec.xyz	ad.evotec.xyz		{CDAB8503-1218-4896-BE52-C5E371896A17}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{CDAB8503-1218-4896-BE52-C5E371896A17}	CN={CDAB8503-1218-4896-BE52-C5E371896A17},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2020-10-19 10:00:34	2020-10-19 10:00:34	
ALL   Allow use of biometrics	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	{10F0E76E-D985-4FA4-91A4-C2F7603273A4}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{10F0E76E-D985-4FA4-91A4-C2F7603273A4}	CN={10F0E76E-D985-4FA4-91A4-C2F7603273A4},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2018-05-20 23:50:07	2020-11-26 10:24:11	
ALL   Bitlocker Settings	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	{3E27E1A0-357F-46C9-88FD-F2E4834E7AE6}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{3E27E1A0-357F-46C9-88FD-F2E4834E7AE6}	CN={3E27E1A0-357F-46C9-88FD-F2E4834E7AE6},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2018-08-07 12:22:23	2020-05-13 20:24:10	
ALL   Certificates	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	{2076528B-C1A1-4201-8BA6-D620A70E0356}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{2076528B-C1A1-4201-8BA6-D620A70E0356}	CN={2076528B-C1A1-4201-8BA6-D620A70E0356},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2020-06-06 20:09:36	2020-09-17 08:52:32	
ALL   Enable RDP	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	{0518C0DF-D011-427B-80FD-68403A630209}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{0518C0DF-D011-427B-80FD-68403A630209}	CN={0518C0DF-D011-427B-80FD-68403A630209},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2018-08-07 12:47:44	2020-12-06 10:19:36	
ALL   Firewall Settings	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	{617EEA5-1606-4330-8009-60DE14823047}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{617EEA5-1606-4330-8009-60DE14823047}	CN={617EEA5-1606-4330-8009-60DE14823047},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2018-08-07 16:42:25	2020-11-11 13:29:04	
ALL   Trusted Websites	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	{37CC53AA-5298-4C09-8977-3F3778269FC8}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{37CC53AA-5298-4C09-8977-3F3778269FC8}	CN={37CC53AA-5298-4C09-8977-3F3778269FC8},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2020-05-09 10:03:32	2020-05-09 10:16:43	
ALL   Windows PowerShell	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	{810F1158-2225-4919-AC72-086079170070}	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{810F1158-2225-4919-AC72-086079170070}	CN={810F1158-2225-4919-AC72-086079170070},CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz		2020-08-27 11:48:10	2020-08-27 11:49:44	

Showing 1 to 10 of 54 entries

Steps to fix - Not available on SYSVOL / Active Directory / ObjectClass issue

Prepare environment | Prepare report | Make a backup (optional) | Fix GPOs not available in AD | Fix GPOs not available on SYSVOL | Fix GPOs of wrong ObjectClass | Verification report

To be able to execute actions in automated way please install required modules. Those modules will be installed straight from Microsoft PowerShell Gallery.

1. Install-Module GPOZaurr -Force
2. Import-Module GPOZaurr -Force

Using force makes sure newest version is downloaded from PowerShellGallery regardless of what is currently installed. Once installed you're ready for next step.

Previous Next

With just a few simple steps, you can have that fixed in a couple of minutes. Keep in mind that you need to have healthy replication of group policies for this to work and not report false positives. If you have unhealthy replication and wrong, DC will get asked about those issues you could potentially remove legitimate content.

### Invoke-GPOZaurr - Report GPOBrokenLink

When GPO is deleted correctly, it usually is removed from AD, SYSVOL, and any link to it is also discarded. Unfortunately, this is true only if the GPO is created and linked within the same domain. If GPO is linked in another domain, this leaves a broken link hanging on before it was linked. Additionally, the Remove-GPO cmdlet doesn't handle site link deletions, which causes dead links to be stuck on sites until those are manually deleted. This means that any GPOs deleted using PowerShell may leave a trail.



## Invoke-GPOZaurr -Type GP0BrokenLink

Report generated on 01/24/2021 11:21:15 GPOZaurr - Current/Latest: 0.0.110 at 01/22/2021 12:41:11

When GPO is deleted in a proper way it usually is removed from AD, SYSVOL and any link to it is also discarded. Unfortunately this is true only if the GPO is created and linked within same domain. If GPO is linked in another domain, this leaves a broken link hanging on wherever it was linked before. Additionally Remove-GPO cmdlet doesn't handle site link deletions, which causes dead links to be stuck on sites until those are manually deleted. This means that any GPOs deleted using PowerShell may leave trail.

As it stands currently there are 2 broken links that need to be deleted over 1 unique objects.

**Following domains require actions (permissions required):**

- ad.evotec.pl requires 2 changes.

**Broken Links**

Group Policy Broken Links								
DistinguishedName	CanonicalName	Guid	Enforced	Enabled	ObjectClass	GPDomainDistinguishedName	GP0DistinguishedName	Search
DC=ad,DC=evotec,DC=pl	ad.evotec.pl	40683630-DE34-4788-A60D-78B703A891F5	False	True	domainDNS	DC=ad,DC=evotec,DC=xyz	cn=140683630-DE34-4788-A60D-78B703A891F5,cn=policies,cn=system,DC=ad,DC=evotec,DC=xyz	
DC=ad,DC=evotec,DC=pl	ad.evotec.pl	85718008-0800-46A3-A4FF-2FCA8DA37E2D	False	True	domainDNS	DC=ad,DC=evotec,DC=xyz	cn=85718008-0800-46A3-A4FF-2FCA8DA37E2D,cn=policies,cn=system,DC=ad,DC=evotec,DC=xyz	

Showing 1 to 2 of 2 entries First Previous 1 Next Last

**Steps to remove Broken Links**

Prepare environment Prepare report Remove Broken Links Verification report

Following command when executed, runs internally command that lists all broken links. After finding them all it deletes them according to given criteria.  
Make sure when running it for the first time to run it with **Whatif** parameter as shown below to prevent accidental removal.

```
1. Repair-GPOZaurrBrokenLink -Whatif -Verbose
```

After execution please make sure there are no errors, make sure to review provided output, and confirm that what is about to be changed matches expected data. Once happy with results please follow with command:

```
1. Repair-GPOZaurrBrokenLink -Verbose -LimitProcessing 2
```

This command when executed removes only first X number of links. Keep in mind that 5 broken links on a single Organizational Unit are treated as one. Use LimitProcessing parameter to prevent mass delete and increase the counter when no errors occur. Repeat step above as much as needed increasing LimitProcessing count till there's nothing left. In case of any issues please review and action accordingly.

Previous Next

## Invoke-GPOZaurr - Report GPOOwners

By default, GPO creation is usually maintained by Domain Admins or Enterprise Admins. When GPO is created by Domain Admins or Enterprise Admins group members, the GPO Owner is set to Domain Admins. When GPO is created by a member of Group Policy Creator Owners or other group has delegated rights to create a GPO, the owner of said GPO is not Domain Admins group but is assigned to the relevant user. GPO Owners should be Domain Admins or Enterprise Admins to prevent abuse. If that isn't so, it means the owner can fully control GPO and potentially change its settings in an uncontrolled way. While at the moment of creation of new GPO, it's not a problem, in the long term, it's possible such a person may no longer be admin, yet keep their rights over GPO. As your aware, Group Policies are stored in 2 places. In Active Directory (metadata) and SYSVOL (settings). This means that there are 2 places where GPO Owners exists. This also means that for multiple reasons, AD and SYSVOL can be out of sync when it comes to their permissions, which can lead to uncontrolled ability to modify them. Ownership in Active Directory and Ownership of SYSVOL for said GPO is required to be the same.

## Invoke-GPOZaurr -Type GP00wners

Broken Group Policies | Group Policy Broken Links | **Group Policy Owners** | GPO Permissions Consistency | Duplicate (CNF) Group Policies | 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

By default GPO creation is usually maintained by Domain Admins or Enterprise Admins. When GPO is created by member of Domain Admins or Enterprise Admins group the GPO Owner is set to Domain Admins. When GPO is created by member of Group Policy Creator Owners or other group has delegated rights to create a GPO the owner of said GPO is not Domain Admins but is assigned to relevant user. GPO Owners should be Domain Admins or Enterprise Admins to prevent abuse. If that isn't so it means owner is able to fully control GPO and potentially change it's settings in uncontrolled way. While at the moment of creation of new GPO it's not a problem, in long term it's possible such person may no longer be admin, yet keep their rights over GPO.

As you're aware Group Policies are stored in 2 places. In Active Directory (metadata) and SYSVOL (settings). This means that there are 2 places where GPO Owners exists. This also means that for multiple reasons AD and SYSVOL can be out of sync when it comes to their permissions which can lead to uncontrolled ability to modify them. Ownership in Active Directory and Ownership of SYSVOL for said GPO are required to be the same.

Here's a short summary of **Group Policy Owners**:

- Administrative Owners: 45
- Non-Administrative Owners: 6
- Owners consistent in AD and SYSVOL: 45
- Owners not-consistent in AD and SYSVOL: 6

**Following will need to happen:**

- Group Policies requiring owner change: 2
- Group Policies which can't be fixed (no SYSVOL): 4
- Group Policies unaffected: 45

**Following domains require actions (permissions required):**

- ad.evotec.pl requires 2 changes.
- ad.evotec.xyz requires 0 changes.

**Following domains require fixing using, different methods:**

- ad.evotec.pl requires 3 changes.
- ad.evotec.xyz requires 1 changes.

### Group Policy Owners

Display Name	Domain Name	GUID	Owner	OwnerSid	OwnerType	SysvolOwner	SysvolSid	SysvolType	SysvolPath	IsOwnerConsistent	IsOwnerAdministrative	SysvolExists	DistinguishedName
New Group Policy Object3	ad.evotec.xyz	59A5084F-8A8F-46A7-802F-84FC0D6E9F44	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative				\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{59A5084F-8A8F-46A7-802F-84FC0D6E9F44}	False	False	False	CN={59A5084F-8A8F-46A7-802F-84FC0D6E9F44},CN=Policies,CN=System,DC=ad,DC=evotec,DC=xyz
DC PowerShell Logging	ad.evotec.pl	7112AF81-5C87-4010-808D-C0F11FAF0714	EVOTECPL\Domain Admins	S-1-5-21-3661168273-3820270925-29702495-512	Administrative				\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{7112AF81-5C87-4010-808D-C0F11FAF0714}	False	False	False	CN={7112AF81-5C87-4010-808D-C0F11FAF0714},CN=Policies,CN=System,DC=ad,DC=evotec,DC=pl
DC Configure Time PDC	ad.evotec.pl	24194233-8B82-4302-4533-ABF4F39A2C24	EVOTECPL\Domain Admins	S-1-5-21-3661168273-3820270925-29702495-512	Administrative				\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{24194233-8B82-4302-4533-ABF4F39A2C24}	False	False	False	CN={24194233-8B82-4302-4533-ABF4F39A2C24},CN=Policies,CN=System,DC=ad,DC=evotec,DC=pl
TEST Empty GPO-AD EVOTEC.PL CrossDomain GPO	ad.evotec.pl	EAD83844-113F-4100-977B-D5D121DF4F91	EVOTEC\Enterprise Admins	S-1-5-21-853615985-2870445339-3163598659-519	Administrative				\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{EAD83844-113F-4100-977B-D5D121DF4F91}	False	False	False	CN={EAD83844-113F-4100-977B-D5D121DF4F91},CN=Policies,CN=System,DC=ad,DC=evotec,DC=pl
Default Domain Policy	ad.evotec.pl	31B2F340-016D-1102-945F-00C04F8984F9	EVOTECPL\Domain Admins	S-1-5-21-3661168273-3820270925-29702495-512	Administrative	BUILTIN\Administrators	S-1-5-32-544	WellKnownAdministrative	\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{31B2F340-016D-1102-945F-00C04F8984F9}	False	False	True	CN={31B2F340-016D-1102-945F-00C04F8984F9},CN=Policies,CN=System,DC=ad,DC=evotec,DC=pl
Default Domain Controllers Policy	ad.evotec.pl	6AC1786C-016F-1102-945F-00C04F8984F9	EVOTECPL\Domain Admins	S-1-5-21-3661168273-3820270925-29702495-512	Administrative	BUILTIN\Administrators	S-1-5-32-544	WellKnownAdministrative	\\ad.evotec.pl\SysVol\ad.evotec.pl\Policies\{6AC1786C-016F-1102-945F-00C04F8984F9}	False	False	True	CN={6AC1786C-016F-1102-945F-00C04F8984F9},CN=Policies,CN=System,DC=ad,DC=evotec,DC=pl
Default Domain Policy	ad.evotec.xyz	31B2F340-016D-1102-945F-00C04F8984F9	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{31B2F340-016D-1102-945F-00C04F8984F9}	True	True	True	CN={31B2F340-016D-1102-945F-00C04F8984F9},CN=Policies,CN=System,DC=ad,DC=evotec,DC=xyz
Default Domain Controllers Policy	ad.evotec.xyz	6AC1786C-016F-1102-945F-00C04F8984F9	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{6AC1786C-016F-1102-945F-00C04F8984F9}	True	True	True	CN={6AC1786C-016F-1102-945F-00C04F8984F9},CN=Policies,CN=System,DC=ad,DC=evotec,DC=xyz
DC Event Log Settings	ad.evotec.xyz	4E1F9C70-1D08-4486-8BA3-144E077084B	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{4E1F9C70-1D08-4486-8BA3-144E077084B}	True	True	True	CN={4E1F9C70-1D08-4486-8BA3-144E077084B},CN=Policies,CN=System,DC=ad,DC=evotec,DC=xyz
DC Event Log Audit Rules	ad.evotec.xyz	55FB3860-74C9-4262-AD77-30197EAB9999	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative	EVOTEC\Domain Admins	S-1-5-21-853615985-2870445339-3163598659-512	Administrative	\\ad.evotec.xyz\SysVol\ad.evotec.xyz\Policies\{55FB3860-74C9-4262-AD77-30197EAB9999}	True	True	True	CN={55FB3860-74C9-4262-AD77-30197EAB9999},CN=Policies,CN=System,DC=ad,DC=evotec,DC=xyz

Showing 1 to 10 of 51 entries

Steps to fix Group Policy Owners

Prepare environment | Prepare report | Make a backup (optional) | **Set GPO Owners to Administrative (Domain Admins)** | Verification report

Following command will find any GPO which doesn't have proper GPO Owner (be it due to inconsistency or not being Domain Admin) and will enforce new GPO Owner. Make sure when running it for the first time to run it with **Whatif** parameter as shown below to prevent accidental removal.

```
1. Set-GPOZaurOwner -Type All -Verbose -Whatif
```

Alternatively for multi-domain scenario, if you have limited Domain Admin credentials to a single domain please use following command:

```
1. Set-GPOZaurOwner -Type All -Verbose -Whatif -IncludeDomains 'YourDomainYouHavePermissionsFor'
```

After execution please make sure there are no errors, make sure to review provided output, and confirm that what is about to be changed matches expected data.

Once happy with results please follow with command (this will start fixing process):

```
1. Set-GPOZaurOwner -Type All -Verbose -LimitProcessing 2
```

Alternatively for multi-domain scenario, if you have limited Domain Admin credentials to a single domain please use following command:

```
1. Set-GPOZaurOwner -Type All -Verbose -LimitProcessing 2 -IncludeDomains 'YourDomainYouHavePermissionsFor'
```

This command when executed sets new owner only on first X non-compliant GPO Owners for AD/SYSVOL. Use LimitProcessing parameter to prevent mass change and increase the counter when no errors occur. Repeat step above as much as needed increasing LimitProcessing count till there's nothing left. In case of any issues please review and action accordingly.

Previous | Next

This report is fairly complete with detection and automated fix.

### Invoke-GPOZaur - Report GPOConsistency

When GPO is created, it creates an entry in Active Directory (metadata) and SYSVOL (content). Two different places mean two different sets of permissions. The group Policy module is making sure the data in both places is correct. However, it's not necessarily the case for different reasons, and often permissions go out of sync between AD and SYSVOL. This test verifies the consistency of policies between AD and SYSVOL in two ways. It checks top-level permissions for a GPO and then checks if all files within said GPO is inheriting permissions or have different permissions in place.

# Invoke-GPOZaurr -Type GPOConsistency

Report generated on 01/23/2021 18:09:07

GPOZaurr - Current/Latest: 0.0.110 at 01/22/2021 12:41:11

Broken Group Policies | Group Policy Broken Links | Group Policy Owners | **GPO Permissions Consistency** | Duplicate (CNF) Group Policies | 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

When GPO is created it creates an entry in Active Directory (metadata) and SYSVOL (content). Two different places means two different sets of permissions. Group Policy module is making sure the data in both places is correct. However, for different reasons it's not necessary the case and often permissions go out of sync between AD and SYSVOL. This test verifies consistency of policies between AD and SYSVOL, in two ways. It checks top level permissions for a GPO, and then checks if all files within said GPO are inheriting permissions or have different permissions in place.

Following list presents **permissions consistency between Active Directory and SYSVOL for Group Policies**

- Top level permissions consistency: 45
- Inherited permissions consistency: 44
- Inconsistent top level permissions: 6
- Inconsistent inherited permissions: 7

Having inconsistent permissions on AD in comparison to those on SYSVOL can lead to uncontrolled ability to modify them. Please notice that if **Not available** is visible in the table you should first fix related, more pressing issue, before fixing permissions inconsistency.

### Permissions Consistency

Category	Consistent	Inconsistent
Top Level	45	6
Inherited	44	7

Display Name	Domain Name	ACL Consistent	ACL Consistent Inside	Owner	Path	SysVol Path	Id	Gpo Status	Description	Creation Time	Modification Time	User Version	Computer Version
TEST   Registry GPOs	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=01446204-0285-420A-4339-500F4F277BC, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{01446204-0285-420A-4339-500F4F277BC}	01446204-0285-420A-4339-500F4F277BC	AllSettingsDisabled		2020-07-15 08:28:29	2020-11-08 10:45:12		
ALL   Enable RDP	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=0518CDDF-CC11-4278-80F0-684C0A6E30DB, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{0518CDDF-CC11-4278-80F0-684C0A6E30DB}	0518CDDF-CC11-4278-80F0-684C0A6E30DB	AllSettingsEnabled		2018-08-07 12:47:44	2020-12-06 10:19:36		
COMPUTERS   Add Administrator	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=08784F69-C541-420F-80FD-EE8ED133910, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{08784F69-C541-420F-80FD-EE8ED133910}	08784F69-C541-420F-80FD-EE8ED133910	AllSettingsEnabled		2020-06-26 13:03:16	2020-06-26 14:42:14		
TEST   Password Filter	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=0D003B13-34F7-48C5-8C3E-38D39668343E, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{0D003B13-34F7-48C5-8C3E-38D39668343E}	0D003B13-34F7-48C5-8C3E-38D39668343E	AllSettingsEnabled		2020-07-31 14:42:42	2020-07-31 21:13:48		
TEST   Local Users and Groups	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=1040A6A7-C702-48D4-824B-8FA584F7B066, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{1040A6A7-C702-48D4-824B-8FA584F7B066}	1040A6A7-C702-48D4-824B-8FA584F7B066	UserSettingsDisabled		2020-06-17 13:23:22	2020-11-07 21:45:16		
ALL   Allow use of biometrics	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=119FE76E-0985-4F44-91A4-C2F7830827AA, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{119FE76E-0985-4F44-91A4-C2F7830827AA}	119FE76E-0985-4F44-91A4-C2F7830827AA	UserSettingsDisabled		2018-05-20 23:50:07	2020-11-26 10:24:10		
TEST   Blocker Settings	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=119EFC16-CBF9-43B6-A178-57312A2B4335, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{119EFC16-CBF9-43B6-A178-57312A2B4335}	119EFC16-CBF9-43B6-A178-57312A2B4335	AllSettingsEnabled		2020-07-31 22:13:25	2020-07-31 21:15:16		
TEST   GPOZaurr Permissions Testing	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=119EFAE7-AB10-4854-90F9-44DEFDA0E958, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{119EFAE7-AB10-4854-90F9-44DEFDA0E958}	119EFAE7-AB10-4854-90F9-44DEFDA0E958	AllSettingsEnabled		2020-11-11 21:29:24	2020-12-22 23:52:02		
TEST   Empty GPO Block Admin	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=1B8E5666-33FA-4807-A088-B4E1489C8066, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{1B8E5666-33FA-4807-A088-B4E1489C8066}	1B8E5666-33FA-4807-A088-B4E1489C8066	AllSettingsEnabled		2020-05-06 15:47:17	2020-07-15 07:26:42		
New Group Policy Object	ad.evotec.vyz	True	True	EVOTEC\Domain Admins	cn=1D011660-6649-4151-887E-E24487032776, cn=policies, cn=system, DC=ad, DC=evotec, DC=vyz	\\ad.evotec.vyz\sysvol\ad.evotec.vyz\Policies\{1D011660-6649-4151-887E-E24487032776}	1D011660-6649-4151-887E-E24487032776	AllSettingsEnabled		2020-11-11 10:17:40	2020-11-11 13:13:14		

### Steps to fix - Permissions Consistency

Following steps will guide you how to fix permissions consistency

Prepare environment → Prepare report → **Fix inconsistent permissions** → Fix inconsistent downlevel permissions → Verification report

Following command when executed fixes inconsistent permissions.

Make sure when running it for the first time to run it with **Whatif** parameter as shown below to prevent accidental removal.

Make sure to fill in TargetDomain to match your Domain Admin permission account

```
1. Repair-GPOZaurrPermissionConsistency -IncludeDomains "TargetDomain" -Verbose -Whatif
```

After execution please make sure there are no errors, make sure to review provided output, and confirm that what is about to be deleted matches expected data. Once happy with results please follow with command:

```
1. Repair-GPOZaurrPermissionConsistency -LimitProcessing 2 -IncludeDomains "TargetDomain"
```

This command when executed repairs only first X inconsistent permissions. Use LimitProcessing parameter to prevent mass fixing and increase the counter when no errors occur. Repeat step above as much as needed increasing LimitProcessing count till there's nothing left. In case of any issues please review and action accordingly.

If there's nothing else to be fixed, we can skip to next step step

[Previous](#)
[Next](#)

This report is fairly complete and with an automated fix.

## Invoke-GPOZaurr - Report GPODuplicates

CNF objects, Conflict objects, or Duplicate Objects are created in Active Directory when there is simultaneous creation of an AD object under the same container on two separate Domain Controllers near about the same time or before the replication occurs. This results in a conflict and a CNF (Duplicate) object exhibits the same. While it doesn't necessarily have a huge impact on Active Directory, it's important to keep Active Directory in a proper, healthy state.

## Invoke-GPOZaurr -Type GPODuplicates

Report generated on 01/23/2021 18:09:07 GPOZaurr - Current/Latest: 0.0.110 at 01/22/2021 12:41:11

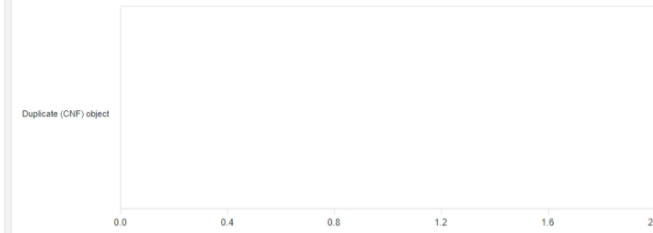
Broken Group Policies    Group Policy Broken Links    Group Policy Owners    GPO Permissions Consistency    **Duplicate (CNF) Group Policies**    Group Policy Summary    Group Policy Links    Group Policy Passwords    Group Policy Permissions Analysis

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

**Duplicate (CNF) Objects**

CNF objects, Conflict objects or Duplicate Objects are created in Active Directory when there is simultaneous creation of an AD object under the same container on two separate Domain Controllers near about the same time or before the replication occurs. This results in a conflict and the same is exhibited by a CNF (Duplicate) object. While it doesn't necessary has a huge impact on Active Directory it's important to keep Active Directory in proper, healthy state. As it stands currently there are 0 CNF (Duplicate) Group Policy objects to be deleted.



Group Policy CNF (Duplicate) Objects

Copy    Excel    CSV    PDF    Show 10 rows    Search:

No data available to display.

Showing 1 to 1 of 1 entries    First    Previous    1    Next    Last

Steps to fix - Remove duplicate (CNF) objects

Prepare environment    Prepare report    **Remove CNF objects**    Verification report

Following command when executed, runs internally command that lists all duplicate objects.  
 Make sure when running it for the first time to run it with **Whatif** parameter as shown below to prevent accidental removal.

```
1. Remove-GPOZaurrDuplicateObject -Whatif -Verbose
```

After execution please make sure there are no errors, make sure to review provided output, and confirm that what is about to be changed matches expected data. Once happy with results please follow with command:

```
1. Remove-GPOZaurrDuplicateObject -Verbose -LimitProcessing 2
```

This command when executed removes only first X duplicate objects. Use LimitProcessing parameter to prevent mass delete and increase the counter when no errors occur. Repeat step above as much as needed increasing LimitProcessing count till there's nothing left. In case of any issues please review and acton accordingly.

Previous    Next

This report is fairly complete and with an automated fix. Be advised above screenshot doesn't show any detected problems because it's pretty hard to generate duplicated objects on-demand, so my test environment doesn't have any. But it does detect those.

### Invoke-GPOZaurr - Report GPOList

Over time Administrators add more and more group policies as business requirements change. Due to neglect or thinking it may serve its purpose, later on, many Group Policies often have no value at all. Either the Group Policy is not linked to anything and 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 groups or persons, 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.

### Invoke-GPOZaurr -Type GPOList

Report generated on 01/23/2021 18:09:07 GPOZaurr - Current/Latest: 0.0.110 at 01/22/2021 12:41:11

Broken Group Policies    Group Policy Broken Links    Group Policy Owners    GPO Permissions Consistency    Duplicate (CNF) Group Policies    **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

Over time Administrators add more and more group policies, as business requirements change. Due to neglect or thinking it may serve its 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: **51**
- Group Policies valid: **14**
- Group Policies **NOT** valid: **37**
  - Group Policies that are unlinked (are not doing anything currently): **30**
  - Group Policies that are empty (have no settings): **17**
  - Group Policies that are linked, but empty: **5**
  - Group Policies that are linked, but link disabled: **1**
  - Group Policies that are disabled (both user/computer sections): **2**
  - Group Policies that have no Apply Permission: **2**
- Group Policies **NOT** valid, to skip: **0** (not older than 7 days)
- Group Policies younger than 7 days: **0** (not older than 7 days)

**Following domains require actions (permissions required):**

- ad.evotec.pl requires **3** changes.
- ad.evotec.xyz requires **34** 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: **3**
  - Group Policies that have content (computer), but are disabled: **2**
  - Group Policies that have content (user), but are disabled: **1**

**Group Policies Empty & Unlinked**



Category	Yes	No
Linked	21	30
Not Empty	34	17
Enabled	49	2
Apply Permission	49	2
Valid	14	37
Optimized (for speed)	4	47
No problem (computers)	48	3
No problem (users)	49	2
Optimized Computers	50	1
Optimized Users	14	37



Such policies require manual review from whoever owns them. It could be a mistake the 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):**

- ad.evotec.pl requires 0 changes.
- ad.evotec.xyz requires 3 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): 26
  - Group Policies that are optimized (user): 14
- Group Policies without optimization:
  - Group Policies that are not optimized (computer): 25
  - Group Policies that are not optimized (user): 37

This means 47 could be optimized for performance reasons.

**Following domains require actions (permissions required):**

- ad.evotec.pl requires 3 changes.
- ad.evotec.xyz requires 44 changes.

**To generate up to date report please execute:**

- Install-Module GPOZaurr -Force or install module manually.
- Invoke-GPOZaurr -FilePath \$Env:UserProfile\Desktop\GPOZaurr\GPOListBefore.html -Verbose -Type GPOList

Steps above will generate above summary with more details allowing you to get up to date report and steps on how to fix it.

**Group Policies List**

Explanation to table columns:

- **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 is no user/computer/group it's applicable to.

Copy   Exclude   CSV   PDF   Show 10 rows   Search:

Display Name	Domain Name	GUID	Days	Empty	Linked	Enabled	Optimized	Problem	Apply Permission	Exclude	Computer Policies	User Policies	Links Count	Links Enabled Count	Links Disabled Count	Enabled Details	Computer Problem	Computer Optimized
TEST   Registry GPOs	ad.evotec.xyz	31445324-4265-409e-e339-56954d278be	76	False	False	False	False	True	True	False	Windows Registry		0	0	0	All settings disabled	True	False
ALL   Enable RCP	ad.evotec.xyz	051bce9f-cc11-427b-b09f-6843eaf36db	48	False	True	True	False	False	True	False	Registry		7	6	1	Enabled	False	True
COMPUTERS   Add Administrator	ad.evotec.xyz	08794f69-c541-429f-b09e-0e630133910	211	False	False	True	False	False	True	False	Local Users and Groups		0	0	0	Enabled	False	True
TEST   Password Filter	ad.evotec.xyz	04d33b15-3477-4bc5-8c3e-3603664343e	175	False	False	True	False	False	True	False	Registry		0	0	0	Enabled	False	True
TEST   Local Users and Groups	ad.evotec.xyz	1946a6a7-c782-486a-824e-8f9d378206e	76	False	False	True	False	True	True	False	Local Users and Groups, Local Users and Services		0	0	0	User configuration settings disabled	False	True
ALL   Allow use of biometrics	ad.evotec.xyz	1095a76e-0905-4f4e-9144-c270308274e	58	False	True	True	True	True	True	False	Name Resolution Policy, Registry		4	3	1	User configuration settings disabled	False	True
TEST   Browser Settings	ad.evotec.xyz	1594e16-c08f-4396-a179-379132b4335	175	False	False	True	False	False	True	False	Registry		0	0	0	Enabled	False	True
TEST   GPOZaurr Permissions Testing	ad.evotec.xyz	19e7ae7-8b10-4854-9209-e446f9a4e58	31	False	True	True	False	False	True	False	Registry		1	1	0	Enabled	False	False
TEST   Empty GPO Block Admin	ad.evotec.xyz	19e79d64-339f-4b07-e089-584149c3066	192	True	False	True	False	False	True	False			0	0	0	Enabled	False	False
New Group Policy Object	ad.evotec.xyz	14011660-6649-4151-827e-c24487032778	73	True	False	True	False	False	True	False			0	0	0	Enabled	False	False

Showing 1 to 10 of 51 entries      First   Previous   1   2   3   4   5   6   Next   Last

**Steps to fix - Empty & Unlinked & Disabled Group Policies**

Following steps will guide you how to remove empty or unlinked group policies

Prepare environment

Prepare report

Make a backup

Excluding Group Policies

Remove GPOs that are EMPTY

Remove GPOs that are UNLINKED

Remove GPOs that are DISABLED

Remove GPOs that do not APPLY

Optimize GPOs (optional)

Verification report

Following command when executed removes every **EMPTY** Group Policy. Make sure when running it for the first time to run it with **WhatIf** parameter as shown below to prevent accidental removal. **Make sure to use BackupPath which will make sure that for each GPO that is about to be deleted a backup is made to folder on a desktop.** You can skip parameters related to backup if you did backup all GPOs prior to running remove command.

```
1. Remove-GPOZaurr -RequireDays ? -Type Empty -BackupPath "$Env:UserProfile\Desktop\GPO" -Verbose -WhatIf
```

Alternatively for multi-domain scenario, if you have limited Domain Admin credentials to a single domain please use following command:

```
1. Remove-GPOZaurr -RequireDays ? -Type Empty -BackupPath "$Env:UserProfile\Desktop\GPO" -Verbose -WhatIf -IncludeDomains 'YourDomainYouHavePermissionsFor'
```

After execution please make sure there are no errors, make sure to review provided output, and confirm that what is about to be deleted matches expected data.

Once happy with results please follow with command (this will start fixing process):

```
1. Remove-GPOZaurr -RequireDays ? -Type Empty -BackupPath "$Env:UserProfile\Desktop\GPO" -LimitProcessing 2 -Verbose
```

Alternatively for multi-domain scenario, if you have limited Domain Admin credentials to a single domain please use following command:

```
1. Remove-GPOZaurr -RequireDays ? -Type Empty -BackupPath "$Env:UserProfile\Desktop\GPO" -LimitProcessing 2 -Verbose -IncludeDomains 'YourDomainYouHavePermissionsFor'
```

This command when executed deletes only first X empty GPOs. Use LimitProcessing parameter to prevent mass delete and increase the counter when no errors occur. Repeat step above as much as needed increasing LimitProcessing count till there's nothing left. In case of any issues please review and action accordingly. Please make sure to check if backup is made as well before going all in.

If there's nothing else to be deleted, we can skip to next step

Previous
Next

This report is fairly complete and provides automated fixes for most issues detected.

### Invoke-GPOZaurr - Report GPOPermissions

The following report contains a full overview of all permissions around Group Policies. It detects 4 different problems (lack of authenticated users, wrong permissions for Domain Admins and Enterprise Admins, Unknown permissions, and lack of proper permission for SYSTEM account). It also contains all permissions, so it's easy to review all permissions from a single place. For each problem, automation is developed, so it's fairly easy to fix any issues as long as you agree with what's proposed.

# Invoke-GPOZaurr -Type GPOPermissions

Report generated on 01/24/2021 11:27:36

GPOZaurr - Current/Latest: 0.0.110 at 01/22/2021 12:41:11

When GPO is created it gets a handful of standard permissions. Those are:

- NT AUTHORITY\Authenticated Users with GpoApply permissions
- Domain Admins and Enterprise Admins with Edit/Delete/Modify permissions
- SYSTEM account with Edit/Delete/Modify permissions

But then IT people change those permissions to their own needs. While most changes make sense and are required to be able to target proper groups of people, some changes are not required or even bad.

### First problem relates to NT AUTHORITY\Authenticated Users

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 [sdlcfe](#) 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.

Unfortunately it's not as simple as it sounds. While checking for permissions mostly works fine, it's possible a Group Policy has totally removed account permissions from being able to assess any of it. The account we use `EVOTEC\PRZEMYSLAK.K205` may simply not have enough permissions to properly assess permissions for a GPO. Therefore we're using dual assessment for this situation, where first assessment is checking for GPO visibility or lack of it, and second assessment is checking for direct permissions assignment. We just were able to detect the problem, but hopefully higher level account (Domain Admin) should be able to provide full assessment.

### First assessment results:

- Group Policies couldn't read at all: 1
- Group Policies with permissions allowing read: 51

### Following domains require actions (permissions required):

- ad.evotec.pl requires 0 changes out of 5.
- ad.evotec.xyz requires 1 changes out of 47.

### Second Assessment results

- Group Policies requiring Authenticated Users with GpoRead permission: 2
- Group Policies which don't require changes: 49

### Following domains require actions (permissions required):

- ad.evotec.pl requires 0 changes.
- ad.evotec.xyz requires 2 changes.

### Second problem relates to Domain Admins and Enterprise Admins

When GPO is created by default it gets Domain Admins and Enterprise Admins with Edit/Delete/Modify Security permissions. For some reason, some Administrators remove those permissions or modify them when they shouldn't touch those at all. Since having Edit/Delete/Modify Security permissions doesn't affect GPOApply permissions there's no reason to remove Domain Admins or Enterprise Admins from permissions, or limit their rights. Domain Admins and Enterprise Admins have to have either GPOEdit/Modify permissions or at the very least GPOCustom. When GPOCustom is set it usually means there's a mix of Allow and Deny permission in place (for example deny GPOApply). In such case we're assuming you know what you're doing. However it's always possible to review those permissions, as those are marked in the table for review.

### Assessment results

- Group Policies requiring Administrative permission fix: 2
- Group Policies which don't require changes: 49

### Following domains require actions (permissions required):

- ad.evotec.pl requires 1 changes.
- ad.evotec.xyz requires 1 changes.

### Third problem relates to SYSTEM account

When GPO is created by default it gets SYSTEM account with Edit/Delete/Modify Security permissions. For some reason, some Administrators remove those permissions or modify them when they shouldn't touch those at all. Since having Edit/Delete/Modify Security permissions doesn't affect GPOApply permissions there's no reason to remove SYSTEM from permissions, or limit their rights.

### Assessment results

- Group Policies requiring SYSTEM permission fix: 1
- Group Policies which don't require changes: 50

### Following domains require actions (permissions required):

- ad.evotec.pl requires 0 changes.
- ad.evotec.xyz requires 1 changes.

### Fourth problem relates to UNKNOWN SID

Sometimes groups or users are deleted in Active Directory and unfortunately their permissions are not cleaned automatically. Those are left in-place and stay there forever until removed.

### Assessment results

- Group Policies requiring Unknown permission removal: 1
- Group Policies which don't require changes: 50

### Following domains require actions (permissions required):

- ad.evotec.pl requires 0 changes.
- ad.evotec.xyz requires 1 changes.

### To generate up to date report please execute:

- Install-Module GPOZaurr -Force or install module manually.
- Invoke-GPOZaurr -FilePath \$env:UserProfile\Desktop\GPOZaurr\GPOPermissionsBefore.html -Verbose -Type GPOPermissions

Steps above will generate above summary with more details allowing you to get up to date report and steps on how to fix it.



Display Name	Domain Name	Permissions Issue	Object Class	Name	Distinguished Name	GUID	When Created	When Changed
ad.evotec.xyz	ad.evotec.pl	True			CN=0478C511-0795-4D1F-8086-E47C19F8295,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz	8478C511-0795-4D1F-8086-E47C19F8295		
TEST   Registry GPOs	ad.evotec.pl	False	groupPolicyContainer	01448204-0285-405A-A539-500F4F279BC	CN=01448204-0285-405A-A539-500F4F279BC,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz	01448204-0285-405A-A539-500F4F279BC	2020-07-15 08:29	2020-11-08 10:44:58
ALL   Enable RDP	ad.evotec.pl	False	groupPolicyContainer	0518C0DF-CC11-4278-B6F0-68C2A4E3008	CN=0518C0DF-CC11-4278-B6F0-68C2A4E3008,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz	0518C0DF-CC11-4278-B6F0-68C2A4E3008	2019-08-07 12:47:44	2020-12-06 10:19:21
COMPUTERS   Add Administrator	ad.evotec.pl	False	groupPolicyContainer	08784F69-C541-423F-82FD-08B3E133910	CN=08784F69-C541-423F-82FD-08B3E133910,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz	08784F69-C541-423F-82FD-08B3E133910	2020-06-26 13:05:16	2020-06-26 15:42:38
TEST   Password Filter	ad.evotec.pl	False	groupPolicyContainer	00033813-347F-48C5-8C3E-38D39A68543E	CN=00033813-347F-48C5-8C3E-38D39A68543E,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz	00033813-347F-48C5-8C3E-38D39A68543E	2020-07-31 14:42:42	2020-07-31 22:13:34
TEST   Local Users and Groups	ad.evotec.pl	False	groupPolicyContainer	104DAA67-C702-48DA-824B-8FA5847838A	CN=104DAA67-C702-48DA-824B-8FA5847838A,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz	104DAA67-C702-48DA-824B-8FA5847838A	2020-06-17 13:23:22	2020-11-07 21:45:01
ALL   Allow use of biometrics	ad.evotec.pl	False	groupPolicyContainer	10F8E76E-0285-4F4A-81A4-C2F7530827AA	CN=10F8E76E-0285-4F4A-81A4-C2F7530827AA,CN=Polices,CN=System,DC=ad,DC=evotec,DC=xyz	10F8E76E-0285-4F4A-81A4-C2F7530827AA	2019-09-20 23:50:07	2020-11-26 10:24:33

Display Name	Domain Name	GUID	Status	Administrative	Authenticated Users	System	Unknown	Domain Admins	Enterprise Admins	Authenticated Users Permission	Domain Admins Permission	Enterprise Admins Permission	System Permission	Unknown Permission
TEST   Registry GPOs	ad.evotec.pl	01448204-0285-405A-A539-500F4F279BC	True	True	True	True	False	True	True	GpoApply	GpoEdit/Delete/Modify/Security	GpoEdit/Delete/Modify/Security	GpoEdit/Delete/Modify/Security	
ALL   Enable RDP	ad.evotec.pl	0518c0df-cc11-4278-b6f0-68c2a4e3008	False	True	False	True	False	True	True		GpoEdit/Delete/Modify/Security	GpoEdit/Delete/Modify/Security	GpoEdit/Delete/Modify/Security	
COMPUTERS   Add Administrator	ad.evotec.pl	08784f69-c541-423f-82fd-08b3e133910	True	True	True	True	False	True	True	GpoApply	GpoEdit/Delete/Modify/Security	GpoEdit/Delete/Modify/Security	GpoEdit/Delete/Modify/Security	



Display Name	GUID	Domain Name	Status	Administrative	Authenticated Users	System	Unknown	Domain Admins	Enterprise Admins	Authenticated Users/Permission	Domain Admins/Permission	Enterprise Admins/Permission	System/Permission	Unknown/Permission
TEST   Password Filter	ad.exeec.rst	4bc5-8c3e-7bc5946343a	True	True	True	True	False	True	True	GpoApply	GpoEnDenyModfySecurity	GpoEnDenyModfySecurity	GpoEnDenyModfySecurity	
TEST   Local Users and Groups	ad.exeec.rst	1346d67-c7d2-4849454d-8fa8d77b2b6	True	True	True	True	False	True	True	GpoApply	GpoEnDenyModfySecurity	GpoEnDenyModfySecurity	GpoEnDenyModfySecurity	
ALL   Allow use of biometrics	ad.exeec.rst	19f5a77e-6955-4f4d-974d-c27f338177a	True	True	True	True	False	True	True	GpoApply	GpoEnDenyModfySecurity	GpoEnDenyModfySecurity	GpoEnDenyModfySecurity	
TEST   BitLocker Settings	ad.exeec.rst	1596f16-c9f9-436d-a17b-57f72a2b4355	True	True	True	True	False	True	True	GpoApply	GpoEnDenyModfySecurity	GpoEnDenyModfySecurity	GpoEnDenyModfySecurity	

Display Name	GUID	Domain Name	Enabled	Description	Creation Date	Modification Time	Permission Type	Permission	Inherited	Principal Name	Principal Distinguished Name	Principal Domain Name	Principal Name	Principal Sid
TEST   Registry GPOs	01446204-c205-4c19-a539-569f4c27f9c	ad.exeec.rst	AllSettingsDisabled		2020-07-15 08:28:29	2020-11-08 10:44:50	Allow	GpoApply	False	NT AUTHORITY\Authenticated Users		ad.exeec.rst	Authenticated Users	S-1-5-11
TEST   Registry GPOs	01446204-c205-4c19-a539-569f4c27f9c	ad.exeec.rst	AllSettingsDisabled		2020-07-15 08:28:29	2020-11-08 10:44:50	Allow	GpoEnDenyModfySecurity	False	EVTEC\Domain Admins	CN=Domain Admins,CN=Users,DC=ad.exeec,DC=rst	ad.exeec.rst	Domain Admins	S-1-5-21-853619895-2870445239-3161088059-512
TEST   Registry GPOs	01446204-c205-4c19-a539-569f4c27f9c	ad.exeec.rst	AllSettingsDisabled		2020-07-15 08:28:29	2020-11-08 10:44:50	Allow	GpoEnDenyModfySecurity	False	EVTEC\Enterprise Admins	CN=Enterprise Admins,CN=Users,DC=ad.exeec,DC=rst	ad.exeec.rst	Enterprise Admins	S-1-5-21-853619895-2870445239-3161088059-519
TEST   Registry GPOs	01446204-c205-4c19-a539-569f4c27f9c	ad.exeec.rst	AllSettingsDisabled		2020-07-15 08:28:29	2020-11-08 10:44:50	Allow	GpoApply	False	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS		ad.exeec.rst	ENTERPRISE DOMAIN CONTROLLERS	S-1-5-9
TEST   Registry GPOs	01446204-c205-4c19-a539-569f4c27f9c	ad.exeec.rst	AllSettingsDisabled		2020-07-15 08:28:29	2020-11-08 10:44:50	Allow	GpoEnDenyModfySecurity	False	NT AUTHORITY\SYSTEM		ad.exeec.rst	NT AUTHORITY\SYSTEM	S-1-5-18
ALL   Enable RDP	0513ad6f-c211-4279-b670-684c2a436db	ad.exeec.rst	AllSettingsDisabled		2018-08-07 12:47:44	2020-12-06 10:18:20	Allow	GpoApply	False	EVTEC\Domain Admins	CN=Domain Admins,CN=Users,DC=ad.exeec,DC=rst	ad.exeec.rst	Domain Admins	S-1-5-21-853619895-2870445239-3161088059-512
ALL   Enable RDP	0513ad6f-c211-4279-b670-684c2a436db	ad.exeec.rst	AllSettingsEnabled		2018-08-07 12:47:44	2020-12-06 10:18:20	Allow	GpoEnDenyModfySecurity	False	EVTEC\Domain Admins	CN=Domain Admins,CN=Users,DC=ad.exeec,DC=rst	ad.exeec.rst	Domain Admins	S-1-5-21-853619895-2870445239-3161088059-512

Steps to fix Group Policy Administrative Users

Progress environment
Progress report
Make a backup (optional)
Add Authenticated Users permissions
Add Administrative Groups permissions
Add SYSTEM permissions
Remove UNKNOWN permissions
Verification report

Depending when this report was run you may want to prepare new report before proceeding with fixing Group Policy Authenticated Users. To generate new report please use:

```
Invoke-GPOZaurr -FilePath $Env:UserProfile\Desktop\GPOZaurrGPOPermissionsBefore.html -Verbosity -Type GPOPermissions
```

When executed it will take a while to generate all data and provide you with new report depending on size of environment. GPOs with problems will be those not having any value for Permission/PermissionType columns. Once confirmed that data is still showing issues and requires fixing please proceed with next step.

Alternatively if you prefer working with console you can run:

```
1. # This gets all permissions
2. $AllPermissions = Get-GPOZaurrPermission
3. $AllPermissions | Format-Table
4. # This analyzes permissions
5. $PermissionsAnalysis = Get-GPOZaurrPermissionsAnalysis
6. $PermissionsAnalysis | Format-Table
```

It provides same data as you see in table above just doesn't prettify it for you.

Previous
Next

This report is interactive, meaning clicking on a GPO in one table limits permissions shown in another table. **GPOPermissions** type is kind of ultimate way for you to deal with permissions. I've made one report that covers what 3 different reports were covering before.

```
Invoke-GPOZaurr -Type
GPOPermissionsRead,GPOPermissionsAdministrative,GPOPermissionsUnknown
```

So while you can use the cmdlet above with each type separately – it's easier to use one.

### Invoke-GPOZaurr - advanced usage

**Invoke-GPOZaurr** is basically a wrapper of around 20 or so different GPO cmdlets that I have developed over a period of six months. I was worried that with so many cmdlets being available in my module and my laziness in the documentation, I thought **Invoke-GPOZaurr's** three-step approach (Describe Problem, Provide Data, Offer Solution) was an experiment that I believe will help me manage my GPOs efficiently for years to come. Not everything is completed, but at the current state, it's good enough for release. It allows you to understand where you stand without spending days, weeks, or months of analysis depending on how big your Active Directory is. Of course, this one little command has few more options that allow for different customization options.

```
Invoke-GPOZaurr [[-Type] <string[]>] [[-ExcludeGroupPolicies] <scriptblock>] [-
FilePath <string>] [-PassThru] [-HideHTML] [-HideSteps] [-ShowError] [-ShowWarning]
[-Forest <string>] [-ExcludeDomains <string[]>] [-IncludeDomains <string[]>]
[<CommonParameters>]
```

Using a **Type** parameter, you can ask for one or multiple types. Providing **FilePath** parameter, you can tell **GPOZaurr** where to save created **HTML** file. **PassThru**, on the other hand, is useful to have **HTML** generated and get the output of the reports back to you for future analysis.

```
PS C:\Users\przemyslaw.klys> Invoke-GPOZaurr -FilePath $Env:UserProfile\Desktop\Test.html -PassThru -Type GPOAnalysis,GPOFiles

[i][GPOZaurr] Version [Informative] Current/Latest: 0.0.110 at 01/22/2021 12:41:11
[i][GPOZaurr] Supported types [Informative] Chosen by user: GPOAnalysis, GPOFiles
[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] SYSVOL (NetLogon) Files List
WARNING: Get-GPOZaurrFiles - Access to the path
'\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{8A7BC515-D7FD-4D1F-90B8-E47C15F89295}' is denied.
(UnauthorizedAccessException)
WARNING: Get-GPOZaurrFiles - Access to the path '\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\scripts\YouCantAccess' is denied.
(UnauthorizedAccessException)
[i][End ] SYSVOL (NetLogon) Files List [Time to execute: 0 days, 0 hours, 0 minutes, 2 seconds, 875 milliseconds]
[i][Start] Group Policy Content
[i][End ] Group Policy Content [Time to execute: 0 days, 0 hours, 0 minutes, 14 seconds, 830 milliseconds]
[i][HTML ] Generating HTML report
[i][HTML ] Generating HTML report [Time to execute: 0 days, 0 hours, 0 minutes, 2 seconds, 806 milliseconds]

Name                               Value
----                               -
Version                             Current/Latest: 0.0.110 at 01/22/2021 12:41:11
Settings                             {ShowError, HideSteps, ShowWarning}
GPOFiles                             {Name, ActionRequired, Data, Exclusions...}
GPOAnalysis                           {Name, ActionRequired, Data, Exclusions...}

PS C:\Users\przemyslaw.klys>
```

It's also possible to hide steps to fix a given problem. This can be useful if you're doing an overview for your Client/Management and don't want to show how to fix it.

```
Invoke-GPOZaurr -FilePath $Env:UserProfile\Desktop\Test.html -Type GPOBroken -
HideSteps
```

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 reappear 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

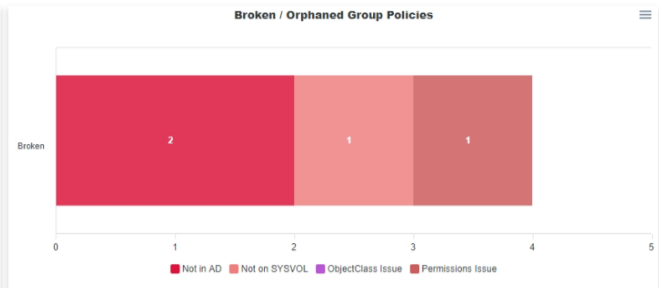
**Following problems were detected:**

- Group Policies on SYSVOL, but no details in AD: 2
- Group Policies in AD, but no content on SYSVOL: 1
- Group Policies which exists, but have wrong ObjectClass: 0
- Group Policies which couldn't be assessed due to permissions issue: 1

**Following domains require actions (permissions required):**

- ad.evotec.pl requires 0 changes.
- ad.evotec.xyz requires 3 changes.

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



Display Name	Status	Domain Name	Sysvol Server	Object Class	ID	Path	Distinguished Name	Description	Creation Time	Modification Time	Error
(28080713-760D-4957-899F-67276DA279E9)	Not available in AD	ad.evotec.xyz	ad.evotec.xyz		(28080713-760D-4957-899F-67276DA279E9)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{28080713-760D-4957-899F-67276DA279E9}	CN={28080713-760D-4957-899F-67276DA279E9},CN=System,DC=ad,DC=evotec,DC=xyz		2020-10-19 10:00:29	2020-10-19 10:00:29	
(8A78C515-07FD-4D1F-408B-E47C15F89295)	Permissions issue	ad.evotec.xyz	ad.evotec.xyz		(8A78C515-07FD-4D1F-408B-E47C15F89295)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{8A78C515-07FD-4D1F-408B-E47C15F89295}	CN={8A78C515-07FD-4D1F-408B-E47C15F89295},CN=System,DC=ad,DC=evotec,DC=xyz				
(C0A8B503-121B-4896-BE52-C9E371984A17)	Not available in AD	ad.evotec.xyz	ad.evotec.xyz		(C0A8B503-121B-4896-BE52-C9E371984A17)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{C0A8B503-121B-4896-BE52-C9E371984A17}	CN={C0A8B503-121B-4896-BE52-C9E371984A17},CN=System,DC=ad,DC=evotec,DC=xyz		2020-10-10 10:00:34	2020-10-10 10:00:34	
ALL   Allow use of biometrics	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	(10F0E74E-0085-4F44-91A4-C2F783027AA)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{10F0E74E-0085-4F44-91A4-C2F783027AA}	CN={10F0E74E-0085-4F44-91A4-C2F783027AA},CN=System,DC=ad,DC=evotec,DC=xyz		2018-05-20 23:50:07	2020-11-26 10:24:03	
ALL   BitLocker Settings	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	(3E07E1AD-357F-46C8-88F0-F2E4834E7AE6)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{3E07E1AD-357F-46C8-88F0-F2E4834E7AE6}	CN={3E07E1AD-357F-46C8-88F0-F2E4834E7AE6},CN=System,DC=ad,DC=evotec,DC=xyz		2018-08-07 12:22:23	2020-05-13 20:23:48	
ALL   Firewall Settings	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	(2C7652B8-C1A1-42C1-8B46-0420A762095A)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{2C7652B8-C1A1-42C1-8B46-0420A762095A}	CN={2C7652B8-C1A1-42C1-8B46-0420A762095A},CN=System,DC=ad,DC=evotec,DC=xyz		2020-06-06 20:09:36	2020-08-17 08:32:28	
ALL   Enable RDP	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	(0518C0DF-CC11-427B-80F0-6440A4E300B)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{0518C0DF-CC11-427B-80F0-6440A4E300B}	CN={0518C0DF-CC11-427B-80F0-6440A4E300B},CN=System,DC=ad,DC=evotec,DC=xyz		2018-08-07 12:47:44	2020-12-06 10:19:21	
ALL   Firewall Settings	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	(617EEA5-1606-4330-8008-600E14823047)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{617EEA5-1606-4330-8008-600E14823047}	CN={617EEA5-1606-4330-8008-600E14823047},CN=System,DC=ad,DC=evotec,DC=xyz		2018-08-07 16:42:25	2020-11-11 13:28:49	
ALL   Trusted Websites	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	(370C33AA-5298-4C09-8977-3F3776209FC8)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{370C33AA-5298-4C09-8977-3F3776209FC8}	CN={370C33AA-5298-4C09-8977-3F3776209FC8},CN=System,DC=ad,DC=evotec,DC=xyz		2020-05-09 10:09:32	2020-05-09 10:16:10	
ALL   Windows PowerShell	Exists	ad.evotec.xyz	ad.evotec.xyz	groupPolicyContainer	(810F1158-2225-4919-AC72-086079170070)	\\ad.evotec.xyz\SYSVOL\ad.evotec.xyz\Policies\{810F1158-2225-4919-AC72-086079170070}	CN={810F1158-2225-4919-AC72-086079170070},CN=System,DC=ad,DC=evotec,DC=xyz		2020-08-27 11:48:10	2020-08-27 11:49:29	

Using **HideHTML** parameter prevents auto-opening of HTML. It's useful for automation purposes.

Invoke-GPOZaurr -FilePath \$Env:UserProfile\Desktop\Test.html -Type GPOBroken -HideSteps -HideHTML

**Invoke-GPOZaurr - Type GPOAnalysis**

**GPO Analysis** report is one of the coolest ones I've made. It's able to provide a lot of smaller reports that show the content of group policies. Each report is a separate tab. Using **GPO GUI**, you would normally show you similar output, but this one does it globally. If you've ever tried to find all GPOs that map drives, find ones that have script execution – it's the way to go.

Invoke-GPOZaurr -Type GPOAnalysis

```

PowerShell
Windows PowerShell
PS C:\Users\przemyslaw.klys> Invoke-GPOZaurr -Type GPOAnalysis
[i][GPOZaurr] Version [Informative] Current/Latest: 0.0.110 at 01/22/2021 12:41:11
[i][GPOZaurr] Supported types [Informative] Chosen by user: GPOAnalysis
[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] Group Policy Content
[i][End ] Group Policy Content [Time to execute: 0 days, 0 hours, 0 minutes, 15 seconds, 447 milliseconds]
[i][HTML ] Generating HTML report
[i][HTML ] Generating HTML report [Time to execute: 0 days, 0 hours, 0 minutes, 1 seconds, 407 milliseconds]
PS C:\Users\przemyslaw.klys>
    
```

AccountPolicies	Audit	Biometrics	BitLocker	EventLog	EventLogService	InternetCommunicationManagement	LAPS	Lithnet	LocalUsers	LocalGroups	MicrosoftOutlook2016	NetMeeting	Policies	Printers	PrintersPolicies				
PublicKeyPoliciesCertificates	PublicKeyPoliciesAutoEnrollment	PublicKeyPoliciesEFS	PublicKeyPoliciesRootCA	PublicKeyPoliciesEnrollmentPolicy	RegistrySetting	RegistrySettings	RemoteDesktopServices	Scripts	SecurityOptions	SoftwareInstallation	SystemServices	SystemServicesNT	TaskScheduler	UserRightsAssignment	WindowsDefenderExploitGuard	WindowsHelloForBusiness	WindowsPowerShell	InternetExplorerZones	
Display Name	Domain Name	GUID	Gpo Type	ClearTextPassword	LockoutBadCount	LockoutDuration	MaximumPasswordAge	MinimumPasswordAge	MinimumPasswordLength	PasswordComplexity	PasswordHistorySize	ResetLockoutCount	MaxClockSkew	MaxRenewAge					
Default Domain Policy	ad.evotec.yz	3182F34D-014D-11B2-94E7-0004E8994F9	Computer	Disabled	5	35	42	1	7	Enabled	24	35	5	7					
Default Domain Policy	ad.evotec.pl	3182F34D-014D-11B2-94E7-0004E8994F9	Computer	Disabled	0	Not Set	180	0	10	Enabled	10	Not Set	5	7					

AccountPolicies	Audit	Biometrics	BitLocker	EventLog	EventLogService	InternetCommunicationManagement	LAPS	Lithnet	LocalUsers	LocalGroups	MicrosoftOutlook2016	NetMeeting	Policies	Printers	PrintersPolicies				
PublicKeyPoliciesCertificates	PublicKeyPoliciesAutoEnrollment	PublicKeyPoliciesEFS	PublicKeyPoliciesRootCA	PublicKeyPoliciesEnrollmentPolicy	RegistrySetting	RegistrySettings	RemoteDesktopServices	Scripts	SecurityOptions	SoftwareInstallation	SystemServices	SystemServicesNT	TaskScheduler	UserRightsAssignment	WindowsDefenderExploitGuard	WindowsHelloForBusiness	WindowsPowerShell	InternetExplorerZones	
Display Name	Domain Name	GUID	Gpo Type	CreatedTime	ModifiedTime	ReadTime	SecurityDescriptor	FilterDataAvailable	Name	IssuedTo	IssuedBy	ExpirationDate							
ALL Certificates	ad.evotec.yz	207852B8-0141-4201-8BA6-9620A70E0395	Computer	2020-06-06 18:03:36	2020-08-17 06:32:28	2021-01-24 16:50:04	SecurityDescriptor	True	RootCertificate	adcs	adcs	2030-06-06T17:46:40Z							
Copy of ALL Certificates	ad.evotec.yz	CE42D01C-072D-4671-8755-86AF02D54E73	Computer	2020-08-13 09:25:08	2020-08-13 09:52:42	2021-01-24 16:50:07	SecurityDescriptor	True	RootCertificate	AdTrust External CA Root	AdTrust External CA Root	2020-05-30T10:48:38Z							
Copy of ALL Certificates	ad.evotec.yz	CE42D01C-072D-4671-8755-86AF02D54E73	Computer	2020-08-13 09:25:08	2020-08-13 09:52:42	2021-01-24 16:50:07	SecurityDescriptor	True	RootCertificate	adcs	adcs	2030-06-06T17:46:40Z							
Copy of ALL Certificates	ad.evotec.yz	CE42D01C-072D-4671-8755-86AF02D54E73	Computer	2020-08-13 09:25:08	2020-08-13 09:52:42	2021-01-24 16:50:07	SecurityDescriptor	True	IntermediateCACertificate	AdTrust External CA Root	AdTrust External CA Root	2020-05-30T10:48:38Z							
Copy of ALL Certificates	ad.evotec.yz	CE42D01C-072D-4671-8755-86AF02D54E73	Computer	2020-08-13 09:25:08	2020-08-13 09:52:42	2021-01-24 16:50:07	SecurityDescriptor	True	IntermediateCACertificate	AffirmTrust Commercial	AffirmTrust Commercial	2030-12-31T14:06:06Z							
Copy of ALL Certificates	ad.evotec.yz	CE42D01C-072D-4671-8755-86AF02D54E73	Computer	2020-08-13 09:25:08	2020-08-13 09:52:42	2021-01-24 16:50:07	SecurityDescriptor	True	TrustedPeopleCertificate	AdTrust External CA Root	AdTrust External CA Root	2020-05-30T10:48:38Z							
Copy of ALL Certificates	ad.evotec.yz	CE42D01C-072D-4671-8755-86AF02D54E73	Computer	2020-08-13 09:25:08	2020-08-13 09:52:42	2021-01-24 16:50:07	SecurityDescriptor	True	TrustedPeopleCertificate	AffirmTrust Commercial	AffirmTrust Commercial	2030-12-31T14:06:06Z							
Copy of ALL Certificates	ad.evotec.yz	CE42D01C-072D-4671-8755-86AF02D54E73	Computer	2020-08-13 09:25:08	2020-08-13 09:52:42	2021-01-24 16:50:07	SecurityDescriptor	True	UntrustedCertificate	AdTrust External CA Root	AdTrust External CA Root	2020-05-30T10:48:38Z							
Copy of ALL Certificates	ad.evotec.yz	CE42D01C-072D-4671-8755-86AF02D54E73	Computer	2020-08-13 09:25:08	2020-08-13 09:52:42	2021-01-24 16:50:07	SecurityDescriptor	True	UntrustedCertificate	AffirmTrust Commercial	AffirmTrust Commercial	2030-12-31T14:06:06Z							

AccountPolicies	Audit	Biometrics	BitLocker	EventLog	EventLogService	InternetCommunicationManagement	LAPS	Lithnet	LocalUsers	LocalGroups	MicrosoftOutlook2016	NetMeeting	Policies	Printers	PrintersPolicies				
PublicKeyPoliciesCertificates	PublicKeyPoliciesAutoEnrollment	PublicKeyPoliciesEFS	PublicKeyPoliciesRootCA	PublicKeyPoliciesEnrollmentPolicy	RegistrySetting	RegistrySettings	RemoteDesktopServices	Scripts	SecurityOptions	SoftwareInstallation	SystemServices	SystemServicesNT	TaskScheduler	UserRightsAssignment	WindowsDefenderExploitGuard	WindowsHelloForBusiness	WindowsPowerShell	InternetExplorerZones	
Display Name	Domain Name	GUID	Gpo Type	PolicyName	PolicyState	PolicyCategory	PolicySupported	PolicyExplain	PolicyText	PolicyCheckbox	PolicyDropDownList	PolicyEditText	Filters	Linked	LinksCount	Links			
DC Event Log Settings	ad.evotec.yz	4E1F9C70-100B-4486-88A3-1448E07F0B4B	Computer	Control the location of the log file	Enabled	Windows Components/Event Log Service/Application	At least Windows Vista	This policy setting controls the location of the log file. The location of the file must be writable by the Event Log service and should only be accessible to administrators. If you enable this policy setting, the Event Log uses the path specified in this policy setting. If you disable or do not configure this policy setting, the Event Log uses the folder %SYSTEMROOT%\system32\winevt\logs.				EditText	True	1	1	ad.evotec.yz\Domain Controllers			
DC Event Log Settings	ad.evotec.yz	4E1F9C70-100B-4486-88A3-1448E07F0B4B	Computer	Back up log automatically when full	Enabled	Windows Components/Event Log Service/Security	At least Windows Vista	This policy setting controls Event Log behavior when the log file reaches its maximum size and takes effect only if the "Retain old events" policy setting is enabled. If you enable this policy setting and the "Retain old events" policy setting is enabled, the Event Log file is automatically closed and renamed when it is full. A new file is then started. If you disable this policy setting and the "Retain old events" policy setting is enabled, new events are discarded and old events are retained. If you do not configure this policy setting and the "Retain old events" policy setting is enabled, new events are discarded and the old events are retained.				True	1	1	ad.evotec.yz\Domain Controllers				
DC Event Log Settings	ad.evotec.yz	4E1F9C70-100B-4486-88A3-1448E07F0B4B	Computer	Specify the maximum log file size (KB)	Enabled	Windows Components/Event Log Service/Security	At least Windows Vista	This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 01 megabytes (2048 kilobytes) and 2 terabytes (2147483647 kilobytes), in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog, and it defaults to 20 megabytes.				True	1	1	ad.evotec.yz\Domain Controllers				
ALL Allow use of biometrics	ad.evotec.yz	10F0E7E6-D985-4FA6-9144-C2F730827AA	Computer	Allow domain users to log on using biometrics	Enabled	Windows Components/Biometrics	At least Windows Server 2008 R2 or Windows 7	This policy setting determines whether users with a domain account can log on or elevate User Account Control (UAC) permissions using biometrics. If you enable or do not configure this policy setting, Windows allows domain users to log on to a domain-joined computer using biometrics. If you disable this policy setting, Windows prevents domain users from logging on to a domain-joined computer using biometrics. Note: Prior to Windows 10, not configuring this policy setting would have prevented domain users from using biometrics to log on.				True	2	2	ad.evotec.yz\Domain Controllers ad.evotec.yz				
ALL Allow use of biometrics	ad.evotec.yz	10F0E7E6-D985-4FA6-9144-C2F730827AA	Computer	Use a hardware security device	Enabled	Windows Components/Windows Hello for Business	At least Windows 10	A Trusted Platform Module (TPM) provides additional security benefits over software because data protected by it cannot be used on other devices. If you enable this policy setting, Windows Hello for Business provisions only occurs on devices with usable 1.2 or 2.0 TPMs. You can optionally exclude security devices, which prevents Windows Hello for Business provisioning from using those devices. If you disable or do not configure this policy setting, the TPM is still preferred, but all devices may provision Windows Hello for Business using software if the TPM is non-functional or unavailable.	Text	Checkbox		True	2	2	ad.evotec.yz\Domain Controllers ad.evotec.yz				
ALL Allow use of biometrics	ad.evotec.yz	10F0E7E6-D985-4FA6-9144-C2F730827AA	Computer	Use biometrics	Enabled	Windows Components/Windows Hello for Business	At least Windows 10	Windows Hello for Business enables users to use biometric gestures, such as face and fingerprints, as an alternative to the PIN gesture. However, users must still configure a PIN to use in case of failures. If you enable or do not configure this policy setting, Windows Hello for Business allows the use of biometric gestures. If you disable this policy setting, Windows Hello for Business prevents the use of biometric gestures. NOTE: Disabling this policy prevents the user of biometric gestures on the device for all account types.	True		True	2	2	ad.evotec.yz\Domain Controllers ad.evotec.yz					
ALL Allow use of biometrics	ad.evotec.yz	10F0E7E6-D985-4FA6-9144-C2F730827AA	Computer	Use Windows Hello for Business	Enabled	Windows Components/Windows Hello for Business	At least Windows 10	Windows Hello for Business is an alternative method for signing into Windows using your Active Directory or Azure Active Directory account that can replace passwords, Smart Cards, and Virtual Smart Cards. If you enable this policy, the device provisions Windows Hello for Business using keys or certificates for all users. If you disable this policy setting, the device does not provision Windows Hello for Business for any user. If you do not configure this policy setting, users can provision Windows Hello for Business as a convenience credential that encrypts their domain	Checkbox		True	2	2	ad.evotec.yz\Domain Controllers					

DisplayName	DomainName	GUID	GpoType	Type	Command	Parameters	Order	RunOrder	Filters	Linked	LinksCount	Links
TEST   Testing SCRIPTS	ad.evotec.xyz	E68C26CF-48CD-4F7E-AF53-8FC10B170E0E	Computer	Startup	test.ps1		0	PSNotConfigured		False	0	
TEST   Testing SCRIPTS	ad.evotec.xyz	E68C26CF-48CD-4F7E-AF53-8FC10B170E0E	Computer	Startup	test4.ps1		1	PSNotConfigured		False	0	
TEST   Testing SCRIPTS	ad.evotec.xyz	E68C26CF-48CD-4F7E-AF53-8FC10B170E0E	Computer	Shutdown	shutdown.bat		0	RunPSSecond		False	0	
TEST   Testing SCRIPTS	ad.evotec.xyz	E68C26CF-48CD-4F7E-AF53-8FC10B170E0E	Computer	Startup	test7.ps1		2	PSNotConfigured		False	0	
TEST   Testing SCRIPTS	ad.evotec.xyz	E68C26CF-48CD-4F7E-AF53-8FC10B170E0E	Computer	Shutdown	shutdown1.ps1		1	RunPSSecond		False	0	
TEST   Testing SCRIPTS	ad.evotec.xyz	E68C26CF-48CD-4F7E-AF53-8FC10B170E0E	Computer	Shutdown	shutdown2.ps1		2	RunPSSecond		False	0	

Showing 1 to 6 of 6 entries

The idea for every report is that each setting is stored per each line. This sometimes means that if the setting has a potential of 50 options, the report will generate 50 columns. I've not found an easy way to make it readable without custom creating and every report. While I do that for some of the reports, some are totally autogenerated. If you feel something is not covered or require a better report, open up an issue, and we can see what can be done.

### Invoke-GPOZaurr - Automating GPOZaurr to Email

Since I want to keep my group policies healthy at all times, I've developed small automation. This automation deals with one report and sends an email to a ticketing system if there is a problem or sends an update to the AD team that everything is great. This automation uses PSWriteHTML (which is also used to generate **HTML** anyway). I've developed the module where the description on each report is available to use outside of **GPOZaurr** (that's where the **PassThru** parameter is useful).

```
Import-Module GPOZaurr -Force
```

```
$PasswordSecureString = 'passwordSecureString'
```

```
$Types = @(
    @{
        Name      = 'GPOOwners'
        Path      = "$PSScriptRoot\Reports\GPOOwners_$(Get-Date -f yyyy-MM-
dd_HH:mm:ss).html"
        Subject   = '[AD Compliance] Group Policy Owners Issue'
        Ticket    = '[Ticket#2001000](https://linkToChangeRequest)'
        Attach    = $true
    }
    @{
        Name      = 'GPODuplicates'
        Path      = "$PSScriptRoot\Reports\GPODuplicates_$(Get-Date -f yyyy-MM-
dd_HH:mm:ss).html"
        Subject   = '[AD Compliance] Group Policy Duplicate (Conflicting) Objects
Detected'
        Ticket    = '[Ticket#2001000](https://linkToChangeRequest)'
        Attach    = $true
    }
    @{
        Name      = 'NetLogonOwners'
        Path      = "$PSScriptRoot\Reports\NetLogonPermissions_$(Get-Date -f yyyy-MM-
dd_HH:mm:ss).html"
        Subject   = '[AD Compliance] NetLogon Owners Issue'
        Ticket    = '[Ticket#2001000](https://linkToChangeRequest)'
        Attach    = $true
    }
    @{
        Name      = 'GPOConsistency'
        Path      = "$PSScriptRoot\Reports\GPOConsistency_$(Get-Date -f yyyy-MM-
dd_HH:mm:ss).html"
        Subject   = '[AD Compliance] Group Policy Consistency'
        Ticket    = '[Ticket#2001000](https://linkToChangeRequest)'
        Attach    = $true
    }
    # Too big
    @{
        Name      = 'GPOPermissions'
        Path      = "$PSScriptRoot\Reports\GPOPermissions_$(Get-Date -f yyyy-MM-
dd_HH:mm:ss).html"
        Subject   = '[AD Compliance] Group Policy Permissions Analysis'
        Ticket    = '[Ticket#2001000](https://linkToChangeRequest)'
        Attach    = $false
    }
    @{
        Name      = 'GPOList'
        Path      = "$PSScriptRoot\Reports\GPOList_$(Get-Date -f yyyy-MM-
dd_HH:mm:ss).html"
        Subject   = '[AD Compliance] Group Policy Empty & Unlinked & Disabled Cleanup'
        Ticket    = '[Ticket#2001000](https://linkToChangeRequest)'
        Attach    = $false
    }
}
```



```

    @{
        Name      = 'GPOBroken';
        Path      = "$PSScriptRoot\Reports\GPOOrphans_$(Get-Date -f yyyy-MM-
dd_HHmss).html";
        Subject   = '[AD Compliance] Group Policy Orphaned/Broken Cleanup'
        Ticket    = '[Ticket#2001000](https://linkToChangeRequest)'
        Attach    = $true
    }
    @{
        Name      = 'GPOBrokenLink'
        Path      = "$PSScriptRoot\Reports\GPOBrokenLink_$(Get-Date -f yyyy-MM-
dd_HHmss).html"
        Subject   = '[AD Compliance] Group Policy Broken Links'
        Ticket    = '[Ticket#2001000](https://linkToChangeRequest)'
        Attach    = $true
    }
)

foreach ($Type in $Types) {
    $EmailHeaderBadReport = EmailHeader {
        EmailFrom -Address 'EmailFrom@evotec.pl'
        EmailTo -Addresses "przemyslawklys@evotec.pl", 'otherguy@evotec.pl'
        EmailServer -Server 'smtpServer' -SSL -Port 25 -UserName 'login' -Password
$PasswordSecureString -PasswordAsSecure
        EmailOptions -Priority High -DeliveryNotifications Never
        EmailSubject -Subject $Type.Subject
        if ($Type.Attach -eq $true) {
            EmailAttachment -FilePath $Type.Path
        }
    }
    $EmailHeaderGoodReport = EmailHeader {
        EmailFrom -Address 'EmailFrom@evotec.pl'
        EmailTo -Addresses "przemyslawklys@test.pl", 'otherguy@evotec.pl'
        EmailServer -Server 'smtpServer' -SSL -Port 25 -UserName 'login' -Password
$PasswordSecureString -PasswordAsSecure
        EmailOptions -Priority Low -DeliveryNotifications Never
        EmailSubject -Subject $Type.Subject
        if ($Type.Attach -eq $true) {
            EmailAttachment -FilePath $Type.Path
        }
    }
    $ReportOutput = Invoke-GPOZaurr -FilePath $Type.Path -Type $Type.Name -PasThru -
HideHTML -Verbose
    foreach ($Report in $ReportOutput.Keys | Where-Object { $_ -notin 'Version',
'Settings' }) {
        if ($ReportOutput[$Report]['ActionRequired'] -eq $true) {
            Email {
                $EmailHeaderBadReport
                EmailBody {
                    EmailText -Text 'Hello Team,' -LineBreak
                    EmailText -Text "I've found disprepency in our domain that needs
to be fixed and I need your help. " -LineBreak

                    $ReportOutput[$Report]['Summary']
                }
            }
        }
    }
}

```

```

        EmailText -LineBreak
        EmailText -TextBlock {
            "This automation was approved by CAB in $($Type.Ticket). "
            "The goal is to keep Group Policies Healthy at all times! "
            "In case of issues please contact Przemyslaw Klys "
        } -LineBreak
        EmailText -Text 'With regards,'
        EmailText -Text 'Automated Monitoring'

    } -FontSize 10pt
}
} else {
    Email {
        $EmailHeaderGoodReport
        EmailBody {
            EmailText -Text 'Hello Team,' -LineBreak
            EmailText -Text "I've run the report and everything is looking
great. Nothing to do here, but just wanted to say - great job! " -LineBreak

            $ReportOutput[$Report]['Summary']

            EmailText -LineBreak
            EmailText -TextBlock {
                "This automation was approved by CAB in $($Type.Ticket). "
                "The goal is to keep Group Policies Healthy at all times! "
                "In case of issues please contact Przemyslaw Klys "
            } -LineBreak
            EmailText -Text 'With regards,'
            EmailText -Text 'Automated Monitoring'
        } -FontSize 10pt
    }
}
}
}

```

Keep in mind that some of those reports can get really large. For example, the permissions report for 4000 GPOs is about 30MB in size. On the other hand, some other reports are much smaller. This is why there's an option to choose whether to attach a report or not.

### *Summary*

**GPOZaurr** is a huge module. It contains a lot of reports, and just a handful of those are shown here. It's almost **20000** lines of code. It can deal with all sorts of **GPO/SYSVOL/NETLOGON** problems you may have. Feel free to explore. On GitHub, the full source code is available (and somewhat readable – one function per file) and about 40 different examples. Not everything may be easy to understand, but I plan to release more blog posts on different ways to deal with issues. What's important to know is that this module will work just fine with just user credentials. Of course, if you've removed authenticated users from a GPO, some reports will skip it, others will mark it as unavailable, but it does work. Of course, fixing issues will require Domain Admin, but that you can do manually – not even running GPOZaurr as Domain Admin.

The code is published on [GitHub](#)

Issues should be reported on [GitHub](#)

Code is published as a module on [PowerShellGallery](#).

The module is signed with a certificate, like any new modules that I create or update.

```
Install-Module GPOZaurr -Force
```

GO Ahead! Have fun! Make sure to report any issues, or if you feel like something would require covering more ground, let me know. My goal is to have **GPOZaurr** as the only way to deal with **Group Policies**.