gytpol
eyes on policy

Gytpol Validator

System Requirements

Doc: GYT-TEC-003
Release: 5

Total pages:	27

Doc. Title:	Gytpol Validator System Requirements

Doc. No.:	GYT-TEC-003	**Classification:**	Confidential
Revision:	5	**Restriction:**	Gytpol and approved recipients
Date:	27th May 2020	**Customer:**	

Owner:	Tal Kollender	**Reviewers/ Approvers:**	Matthew Album Gilad Raz Tal Kollender
Author:	Tal Kollender		

Contents

Introduction

The purpose of this document is to provide the system requirements and pre-requisites before installing the gytpol Validator product.

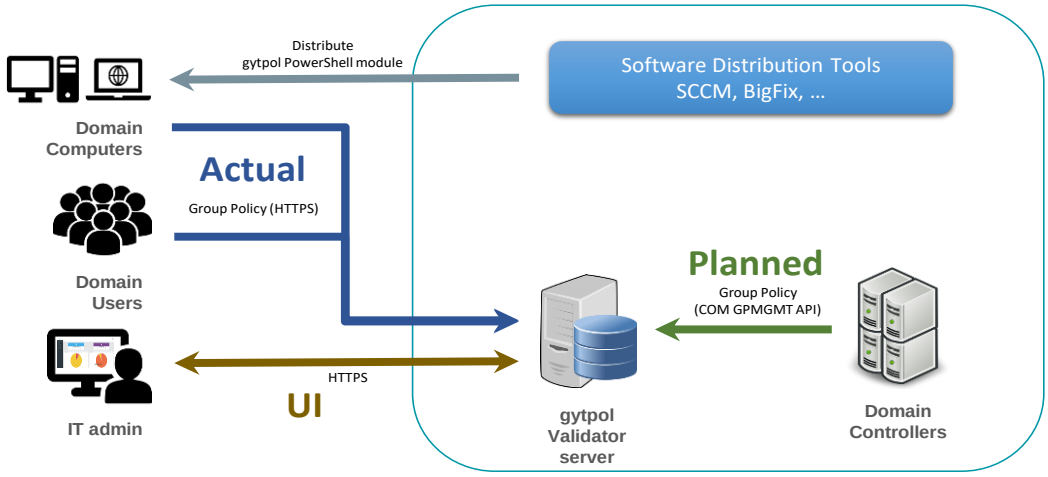
Checklist

Verify all the following gytpol requirements are met prior to installation of the gytpol Validator software:

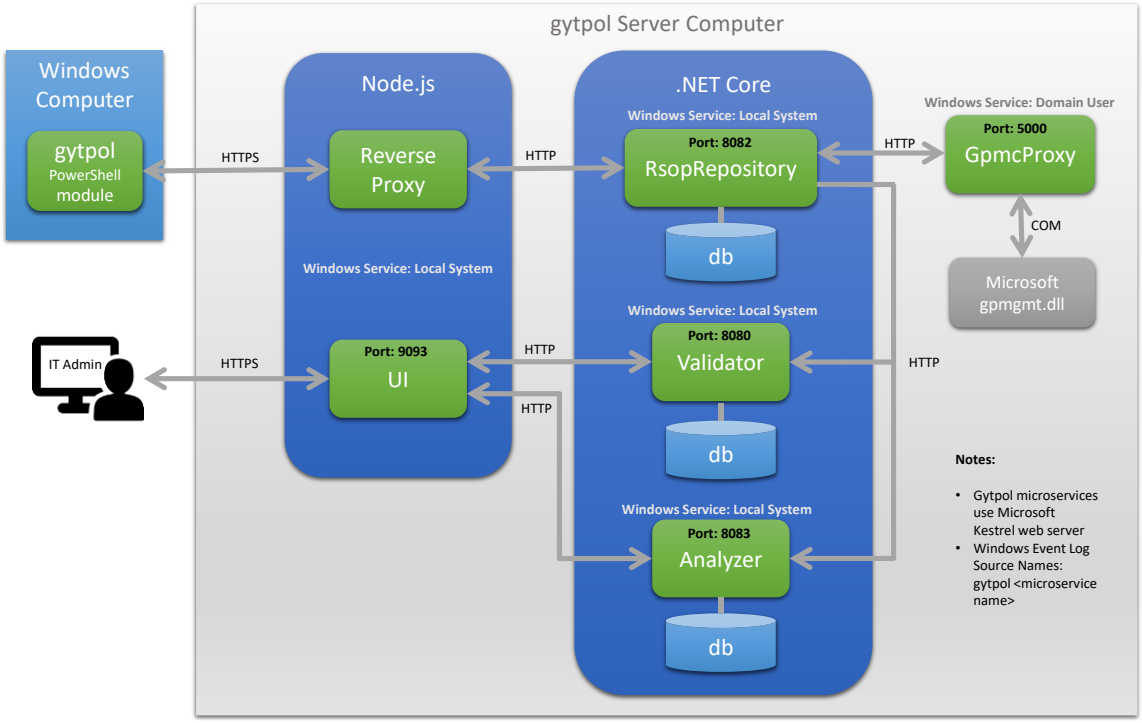
- OS – for the gytpol Server
- Server Sizing – based on number of users and computers
- Users and Groups – in Active Directory and the gytpol Server
- Server Software – for the gytpol Server
- User Interface – web browser for the end user of gytpol Validator
- Client Requirements – for servers and workstations covered by gytpol Validator
- DNS – additions for proper routing to gytpol Server
- Ports – what ports should be open on the server and the client side
- Antivirus – prevent blocking gytpol Validator from proper execution

Find additional help in Appendix: Detailed Configuration Instructions when required.

System Architecture



Server Architecture



OS

- Dedicated physical or virtual server
- OS: Windows Server 2016 (Standard) or Windows Server 2019

Server Sizing

RAM (GB)	System Storage (GB)	CPU (# Cores)
16	80	8

Users and Groups

Domain User and Group in Active Directory

Create in the same domain where gytpol Validator server is located the following objects:

1. Active Directory Domain User (preferred name: **gytpolSvc**) – this user queries the DC and must be a local admin on gytpol server
2. Active Directory Domain Security Group (preferred name: **gytpolAdmins**) – the group is created for security reasons to access gytpol Validator dashboard

Permissions

Follow the table to set the permissions regarding the user and the group:

Type	Name	Permission set
User	gytpolSvc	On the gytpol Server (follow hyperlinks for how to's): • Member of Domain Group: "Performance Log Users" • Local admin on gytpol server • Logon as a service • Logon as a batch job In case of using external DB, like SQL (organizations above 3500 users): • SQL server must be at least version 2016 • DB Creator GPMC permissions
Security Group	gytpolAdmins	• gytpolsvc user should be a member of this group • Add members that should have access to Validator dashboard

Follow the How to Test Permissions instructions.

Server Software

Requirement	How to Verify
Web Browser supports Chromium	Chromium for Edge or Google Chrome version 74 or higher
.NET 4.7.2 installed	
PowerShell minimum version is 5.1 Make sure the PowerShell scripts is not set to “Restricted” in any of its category	How to Check PowerShell Version and Restriction Mode
IPv6 disabled	How to Check if IPv6 is disabled
Windows Firewall is at ‘off’ state (service should be up and running)	How to check if Windows Firewall is at ‘off’ state
IE enhanced disabled	How to Disable Internet Explorer Enhanced Security Configuration
UAC disabled	How to Disable User Account Control (UAC)
Proxy is not configured	How to Disable Proxy Settings
After committed changes - restart the remote machine	

User Interface

- Physical or virtual machine running at least Windows 7 SP1
- Chrome browser running version 74 or later

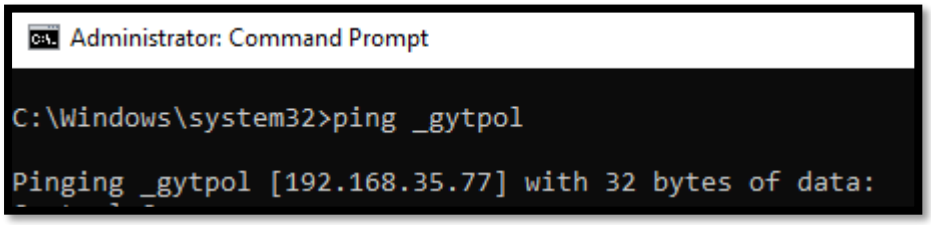
Client Requirements

- Task Scheduler enabled for user and computer
- Event viewer enabled for user and computer
- RSOP allowed
- PowerShell 2.0 or later
    - Recommended: if PowerShell scripts are Restricted, set PowerShell scripts to: “All Signed” (or anything besides “Restricted” or “Remote Sign”, preferred: via GPO)
    - Enable running PS scripts to users

DNS

From a server running DNS (or an IT admin computer):

- Press Start and type Powershell → click on the Windows PowerShell
- Type **dnsmgmt.msc**
- Navigate to the tree name of the organization
- Right click on the tree name → Add **CNAME** Record
- In the name value type **_gytpol**
- In the CNAME record click Search and drill down to the tree level where gytpol server dns name is written and select it → click OK
- Review the results and click OK
- Testing the record:
    - Click start → type cmd → double click to open the cmd windows
    - Type: ping _gytpol
    - Make sure you get the same IP as gytpol server



Ports

From	To	Port number	Purpose
All Computers	gytpol Proxy Server	9093 9090 (Windows7 only)	HTTPS HTTP (data is compressed and encrypted)
gytpol Validator Server	DC's	389, 9389, 636, 135, 138-139, 445, 464, 53, 3268, 3269 + Dynamic ports (49152-65535)	GP PS queries + GP modeling queries
gytpol Validator Server	gytpol Cloud Updates (https://gytpol-cloud-api.azure-api.net/hp/api/v.1.0/)	443	HTTPS (Automatic updates and Remote Employees data pulling) – In case gytpol cloud service connection is desired
gytpol Validator Server	SQL Server	1433	Database – In installations of over 3500 users, SQL server is required
gytpol Validator Server	SIEM Server	2000/514 (whatever works in the organization)	SIEM Integration (ArcSight, QRadar, Splunk, etc.)
IT Admin Computers	gytpol Server	3389 9093	RDP UI – HTTPS

Antivirus

Exclude the following directories in the AV for gytpol server:

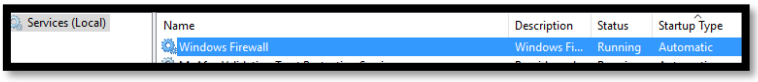
- (gytpol installation directory – i.e. 'C' or 'D' drive):
  LOCAL SERVER\(Local Drive)\gytpol

Appendix: Detailed Configuration Instructions

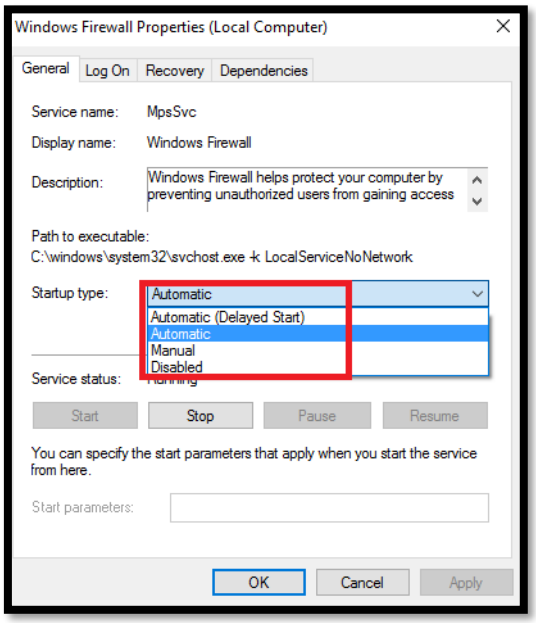
How to check if Windows Firewall is at 'off' state

1. On gytpol server click on "Start" and type Powershell → click on "Windows PowerShell"
2. Type firewall.cpl
3. Make sure the following components are set to "off" (red X):
    - Domain networks
    - Private networks
    - Guest or public networks

4. In case at least one on them is set to "on" (Green)
    a. Click on "Turn Windows Firewall on or off" and change all of the tabs to "off"
5. Type services.msc
6. On the right pane, find the service Windows Firewall and make sure the service is set to Automatic and is running



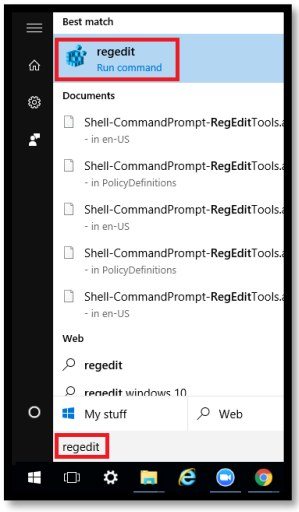
7. If the service is set to stopped and the Startup type is disabled:
    a. Double click on the service and change the startup type to Automatic, click on the Start button and wait for the service to start. After it is done click OK



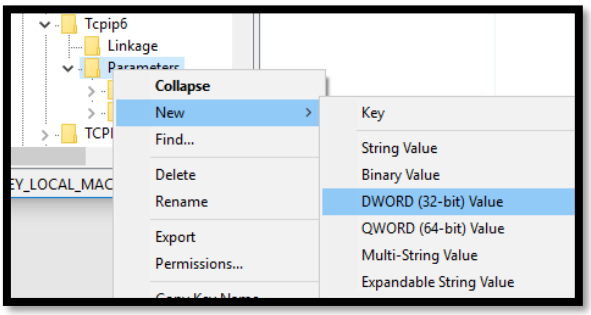
b. If it is unable to change – check the Group Policy in a case the Windows Firewall service is Disabled

How to Check if IPv6 is disabled

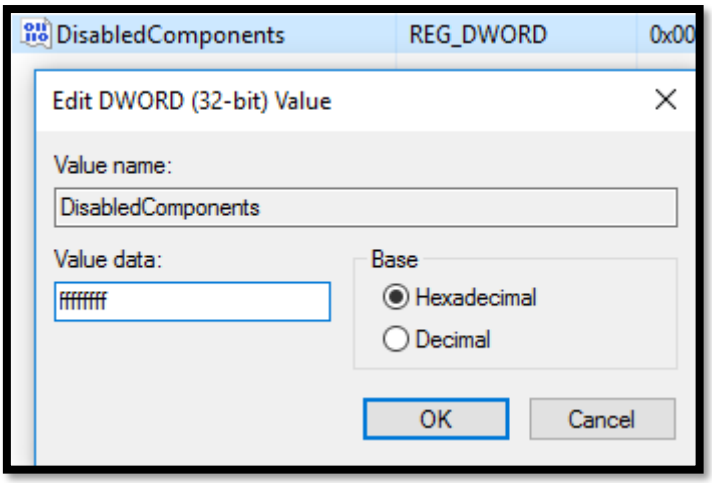
1. In the gytpol server, click on the Start button and type regedit and select the regedit icon:



2. Navigate to HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Services → TCPIP6 → Parameters
3. Right click on Parameters → New → DWORD (32-bit) Value

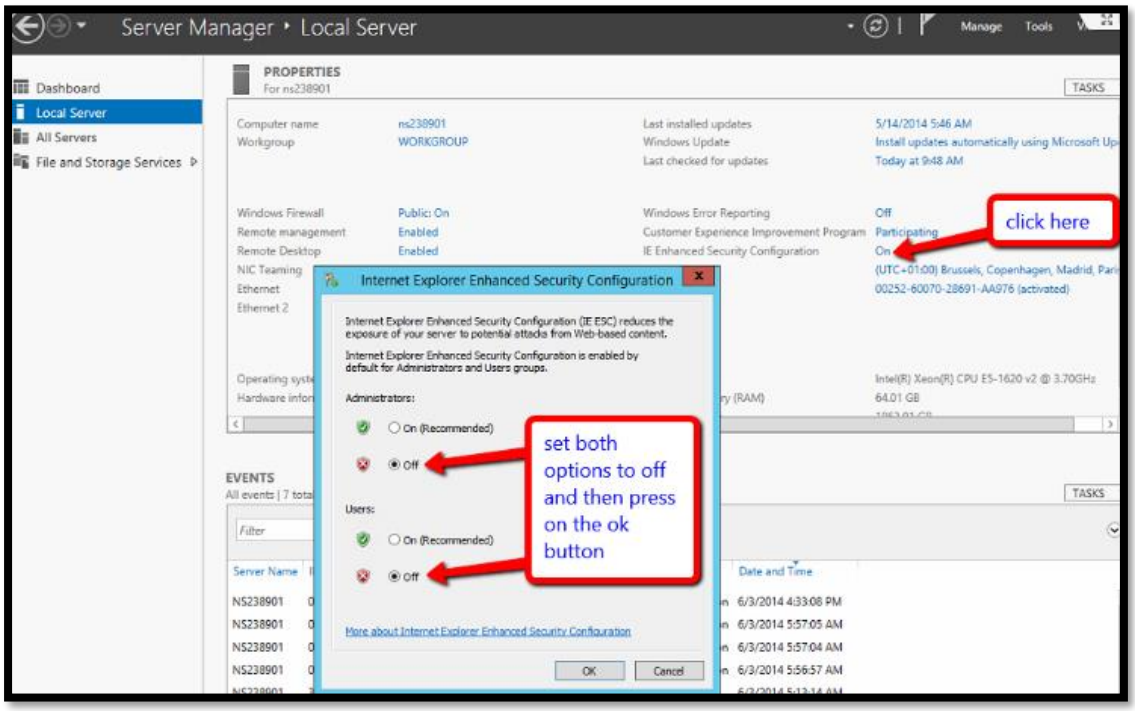


4. Replace the New Value #1 with DisabledComponents
5. Double click on **DisabledComponents** and set the value to **ffffffff** and press OK



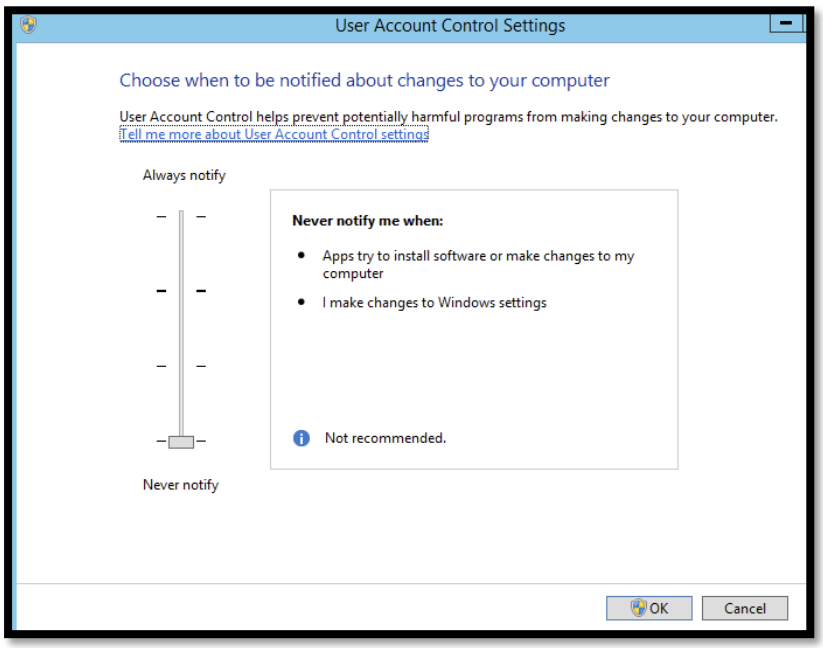
How to Disable Internet Explorer Enhanced Security Configuration

1. On gytpol server click on “Start” and search for Server Manager
2. When the console loads go to Server Manager > Local Server
3. In the Properties section, scroll to the right until you see this option: IE Enhanced Security Configuration, and toggle the setting to Off
4. In the Internet Explorer Enhanced Security Configuration window, disable the IE ESC for Administrators and Users, and click OK



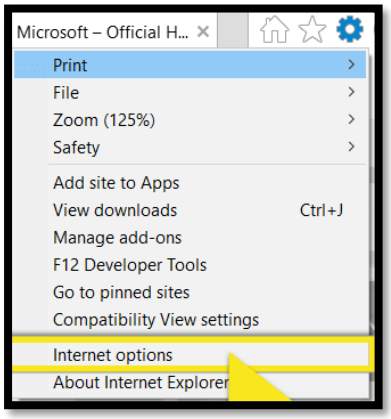
How to Disable User Account Control (UAC)

1. On gytpol server click on “Start” and search for Control Panel
2. When the Control Panel opens → Click System Security
3. Under Action Center, choose Change User Account Control settings
4. Move the slider bar **down** to the **Never notify** selection and click OK
5. Reboot the machine for changes to take effect

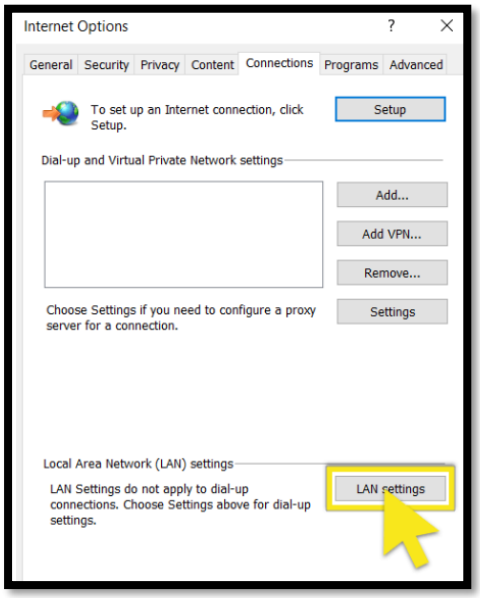


How to Disable Proxy Settings

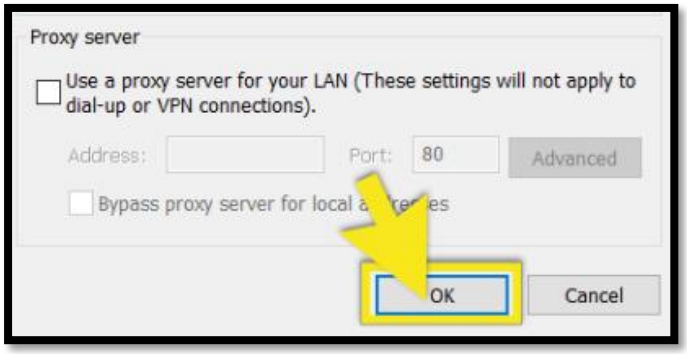
1. On gytpol server click on “Start” and search for Internet Explorer
2. When the Internet Explorer loads → Click the Tools button and then select **Internet Options**



3. Click the **Connections tab** and then select **LAN settings**



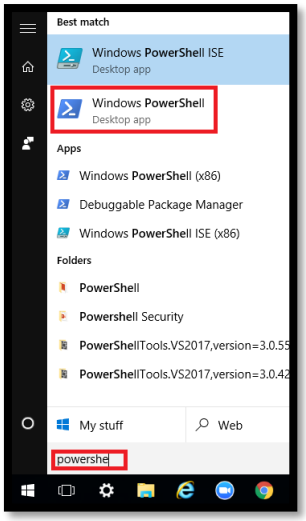
4. Uncheck the check box for Use a proxy server for your LAN



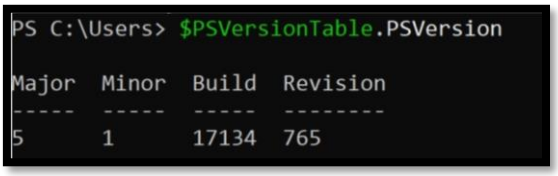
5. Press OK → OK → OK

How to Check PowerShell Version and Restriction Mode

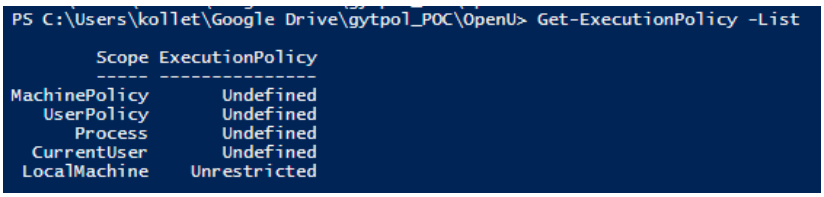
1. On gytpol server click on “Start” and type Powershell → click on “Windows PowerShell”



2. In the WindowsPowerShell window type: **$PSVersionTable.PSVersion**

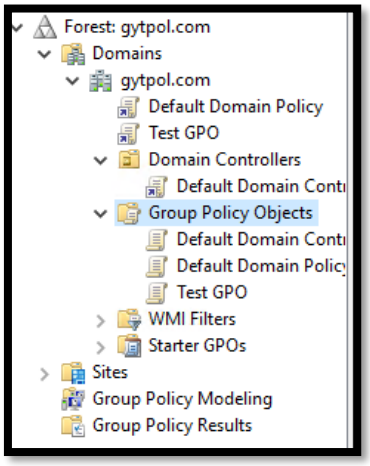


3. Make sure the Major is set to 5 (or above) and the Minor is set to 1 (or above)
4. Make sure the PowerShell scripts is not set to “Restricted” in any of its category: in the same PowerShell windows type: **Get-ExecutionPolicy -List**

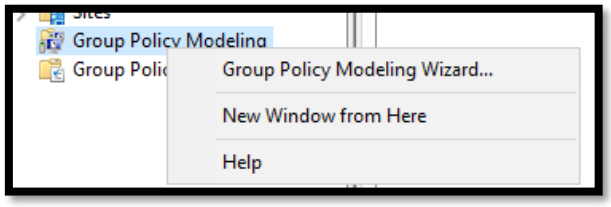


How to Test Permissions

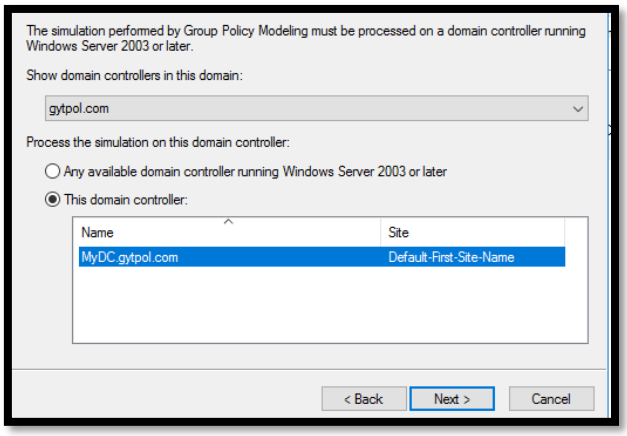
1. Open GPMC.MSC with the user created under section (2)
2. Navigate to “Group Policy Objects” and make sure you see all of the items:



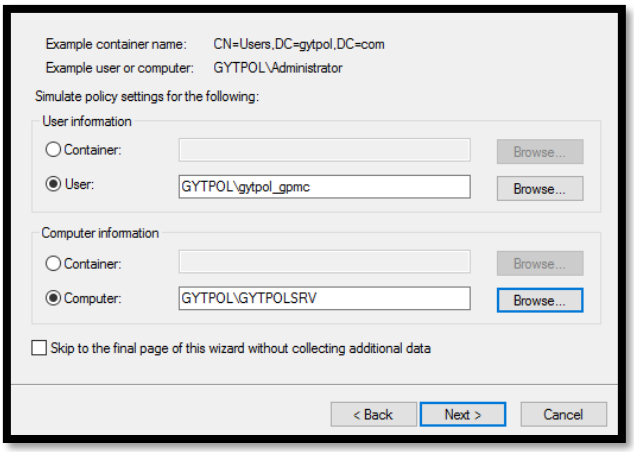
3. If you don’t see the items, open GPMC as administrator and go to Group Policy Objects
    - On the right screen go to Delegation
    - Click “Add..” and choose “gytpolsvc” → OK
4. Navigate to “Group Policy Modeling” and simulate scenario:
    - Right click on the “Group Policy Modeling” → Group Policy Modeling Wizard



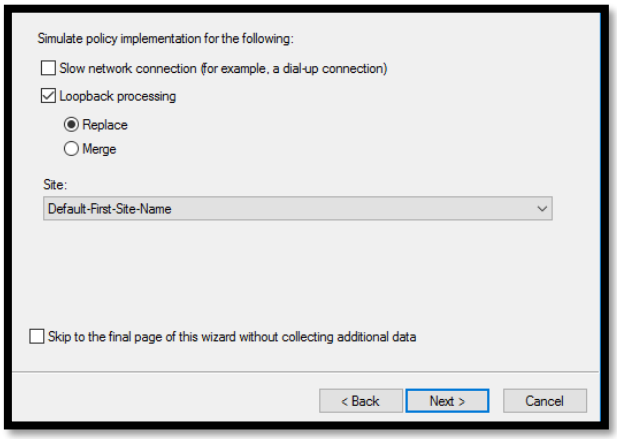
    - Click next → Choose your domain + your PDC server and click next



- Under “User Information” – select “User:” and “Browse..” your username, and under “Computer Information” – select “Computer:” and “Browse..” your computer name → Click next



- Select “Loopback processing” – choose “Replace” and under “Site:” – select your site name → Click next



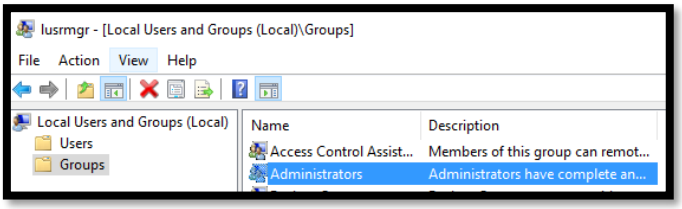
- Continue clicking next until the wizard is finished and review the results

Add the gytpol user to the Domain group: “Performance Log Users”

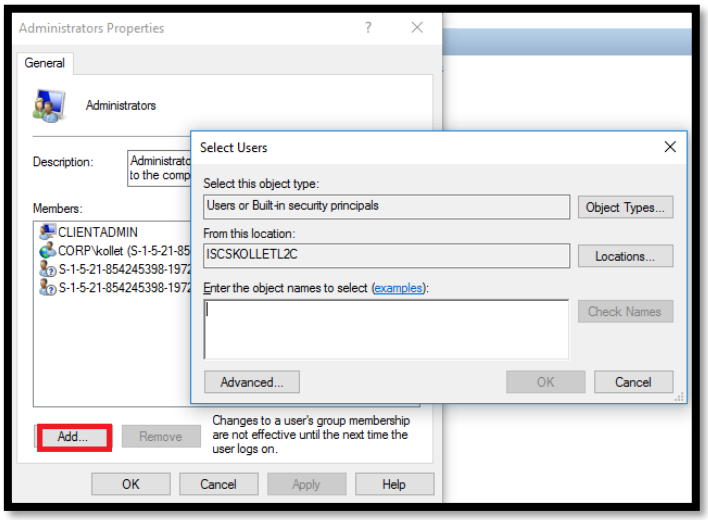
1. From a computer running RSAT (aka Active Directory tools) open cmd
2. Open Active Directory Users and Computers: type dsa.msc and press ENTER
3. Search the Active Directory for the group “Performance Log Users”
4. Double click on the group and go to Members → Add.. → type the name of gytpol user (you created earlier) and press OK → OK → OK

Adding a local admin

5. On **gytpol server** open cmd
6. Type: **lusrmgr.msc**
7. On the left pane select Groups, on the right pane double click on Administrators



8. Click “Add..”



9. Make sure “From this location:” is set to the domain name and not the gytpol server

10. Under “Enter the object names to select” type gytpoSvc → click on “Check Names” and wait until you see the name with underline and with the domain name and press OK

Logon as a service

1. If there are no Group Policies with “logon as a service” restrictions, you might leave it as it is
2. If there are Group Policy with “logon as a service” restriction:
   2.1. Go to a computer where Group Policy Management Console (GPMC) is installed (it is installed by default on all of the Domain Controllers)
   2.2. Open cmd as administrator and type **gpmc.msc**
   2.3. Go to the policy where the restriction is set and right click → edit.
   2.4. Navigate to Computer Configuration → Windows Settings → Security Settings → Local Policies → User Right Assignment
   2.5. Double click on “Log on as a service”
   2.6. Click on “Add User or Group”
   2.7. Type gytpolSvc and click on Check Names
   2.8. Make sure this is the user and click OK

Logon as a batch job

1. If there are no Group Policies with “logon as a batch job” restrictions, you might leave it as it is
2. If there are Group Policy with “logon as a batch job” restriction:
   2.1. Go to a computer where Group Policy Management Console (GPMC) is installed (it is installed by default on all of the Domain Controllers)
   2.2. Open cmd as administrator and type **gpmc.msc**
   2.3. Go to the policy where the restriction is set and right click → edit.
   2.4. Navigate to Computer Configuration → Windows Settings → Security Settings → Local Policies → User Right Assignment
   2.5. Double click on “Log on as a batch job”
   2.6. Click on “Add User or Group”
   2.7. Type gytpolSvc and click on Check Names
   2.8. Make sure this is the user and click OK

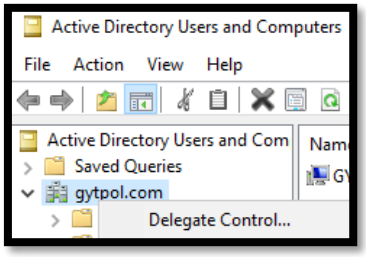
DB Creator

1. Log in to the system using my_domain\my_account or the local system administrator.
2. Log in to SQL Server using administrator (sa) permissions or the local system administrator.
3. Expand the Security folder in the navigation tree.
4. Right-click the Logins folder and select New Login ...
5. Under General on the New Login dialog, complete the following actions:
   5.1. Select Windows Authentication.
   5.2. Click Search, enter a login name (for example, gytpolSvc), then click Check Names.
6. In the dialog, verify the resolved account my_domain\gytpolSvc.
7. Under Server Roles, add the dbcreator role and click OK.
8. The new database user has sufficient privileges to install Server Automation.

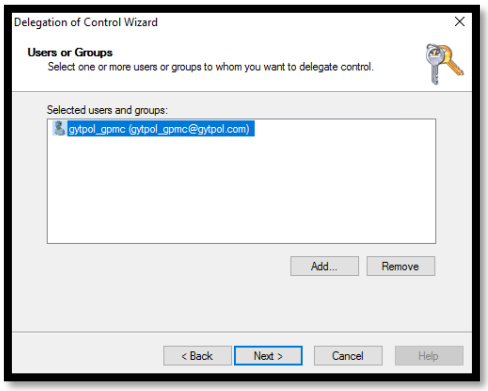
GPMC Permission

Active Directory Delegation

1. Open Active Directory Users and Computers
2. Right click on “yourDomain.com” → Delegation Control:

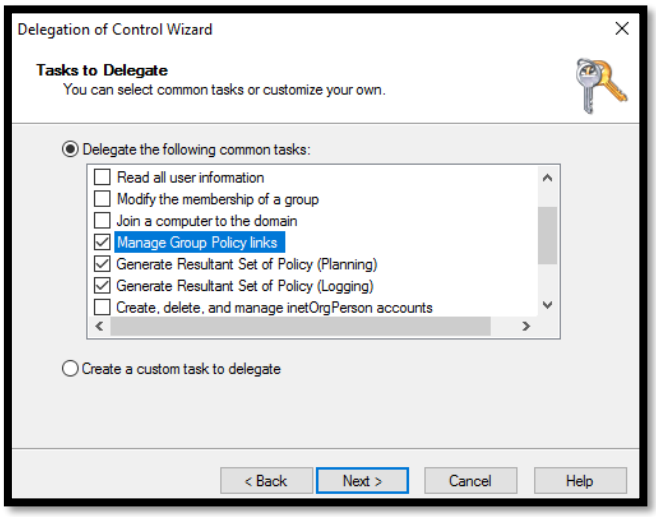


3. Click next → select gytpol user (mentioned in the table below)



4. Click next → Under “Tasks to Delegate” Select the following:

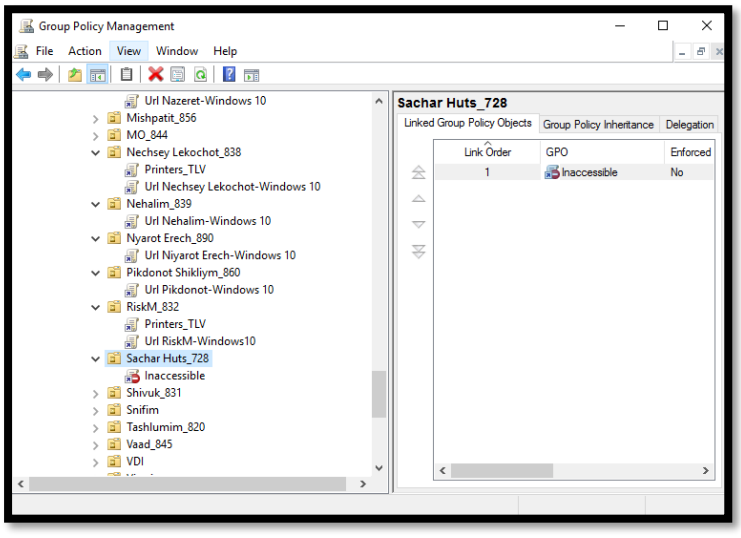
   a) Manage Group Policy links
   b) Generate Resultant Set of Policy (Planning)
   c) Generate Resultant Set of Policy (Logging)



5. Click next and Finish

Group Policy Links Permissions

1. From a server running GPMC (and is not the Domain Controller) – start the GPMC with gytpolSvc user
2. Expand the tree and make sure the user can see all of the linked Group Policies:
3. In case the user has “Inaccessible”:



4. Open the GPMC with a privilege user → navigate to the OU with the Inaccessible group policy link (as a privilege user you should see the name of the policy) → click on that policy → on the right pane navigate to “Delegation” tab

5. On the bottom of the delegation tab press “Add..” → select gytpolSvc (or: Authenticated Users) → click OK
6. In the window after leave it with **Read** permissions and press OK

Make sure you don’t miss any Group Policy Object behind