Gytpol Validator

High Level Architecture

Doc: GYT-TEC-001
Release: 3
Date: 21st May 2020

Confidential: gytpol and approved recipients

Total pages:	13

Doc. Title:	Gytpol Validator High Level Architecture

Doc. No.:	GYT-TEC-001	**Classification:**	Confidential
Revision:	3	**Restriction:**	Gytpol and approved recipients
Date:	21st May 2020	**Customer:**	

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

Contents

Introduction

gytpol Validator is a cyber security software solution, helping IT and Security teams to ensure secure and efficient configuration of their Microsoft Windows platform. The product automates the following use cases:

- Validating that Windows computers and user Group Policies have been correctly applied to all endpoints at all times
- Benchmarking Active Directory and Group Policy configuration versus the industry security standards such as CIS, HIPAA, etc.
- Finding endpoint threats caused by Operating System and 3rd party application misconfiguration (e.g. IIS running on PCs, file shares with excess permissions, left-over SIDs, etc.)
- Optimizing Group Policy definitions (e.g. finding duplicated and conflicting GPOs)
- Identifying Group Policies that are slowing down computer start up time and user login time

This document provides an overview of gytpol Validator technical architecture and major data flows.

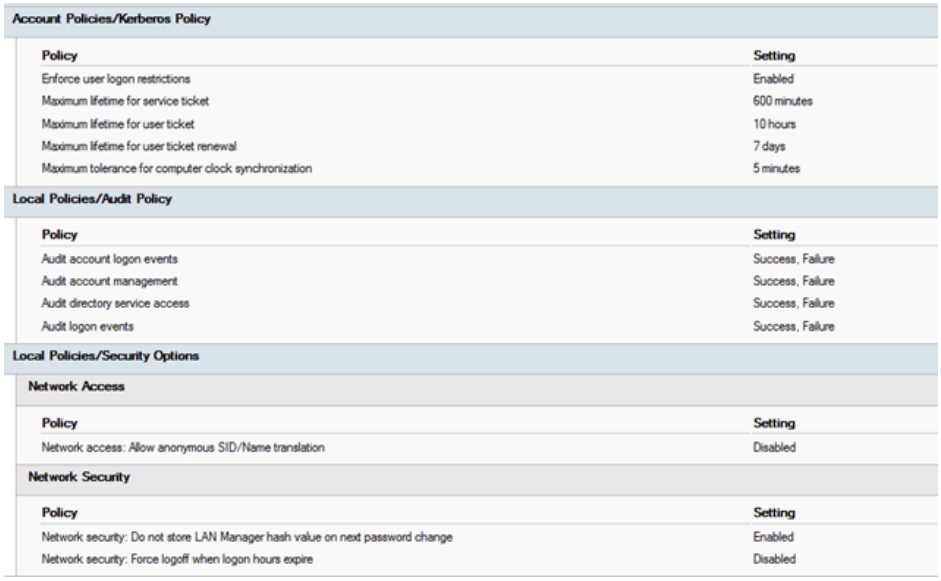
Assumptions

It is assumed that the reader is familiar with Microsoft Group Policy and related software tools, i.e. GPMC, Active Directory, etc. If you are new to Group Policy, we quickly describe it in the next section.

About Microsoft Group Policy

Group Policy is the main, and in many cases the only mechanism to control the configuration of every Windows computer in an organization. It allows what users can and cannot do when using it.

Group Policies are configured in a tool called Group Policy Management Console (GPMC). This is the standard tool provided by Microsoft. GPMC allows you to create and edit Group Policies and configure their Settings. Once Group Policies and Settings are defined, they are applied to various groups of computers and users within my organization.



Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure

Local Policies/Security Options

Network Access

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled

Network Security

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled

Figure 1. Group Policy Settings in GPMC

There are thousands of Settings that control everything ranging from what IE version a user can open, to which locations on the network he can access, down to what would be the desktop wallpaper.

Where a Setting had been modified, the change is supposed to be applied to all relevant computers and users that are set as the target for this policy. But there is no practical way to check that the change actually took place and was effective on all its targets. This comes from a variety of reasons:

1. When creating or modifying a Group Policy, GPMC doesn't give a clear picture of what is the impact of each Setting.
2. There is no indication when a Setting is irrelevant to the OS and other software installed on the targeted computers.
3. A change may not reach a computer or a user for various reasons, e.g. network outages.
4. The policy might have not been properly enabled and applied to the target group.
5. The computer might not be receiving policy updates because of a configuration problem.
6. Some Settings might be conflicting with other settings that were applied by another policy.

How gytpol Validator Works

gytpol Validator is deployed on-premise. A customer should provide a dedicated physical or virtual MS Windows Server for gytpol Validator Server deployment. Please refer to the gytpol Validator System Requirements documents for the exact specifications.

gytpol Validator consists of a **gytpol Client** (a signed PowerShell script) distributed to all relevant MS Windows endpoints in the organization and **gytpol Server**. We discuss gytpol Server and gytpol Client in more details below.

It takes just a few minutes to install the gytpol Server using the installer that leads the user through a series of typical installation questions. The next product deployment step is distributing client installer msi using the organization's software distribution tools such as Microsoft SCCM or IBM BigFix.

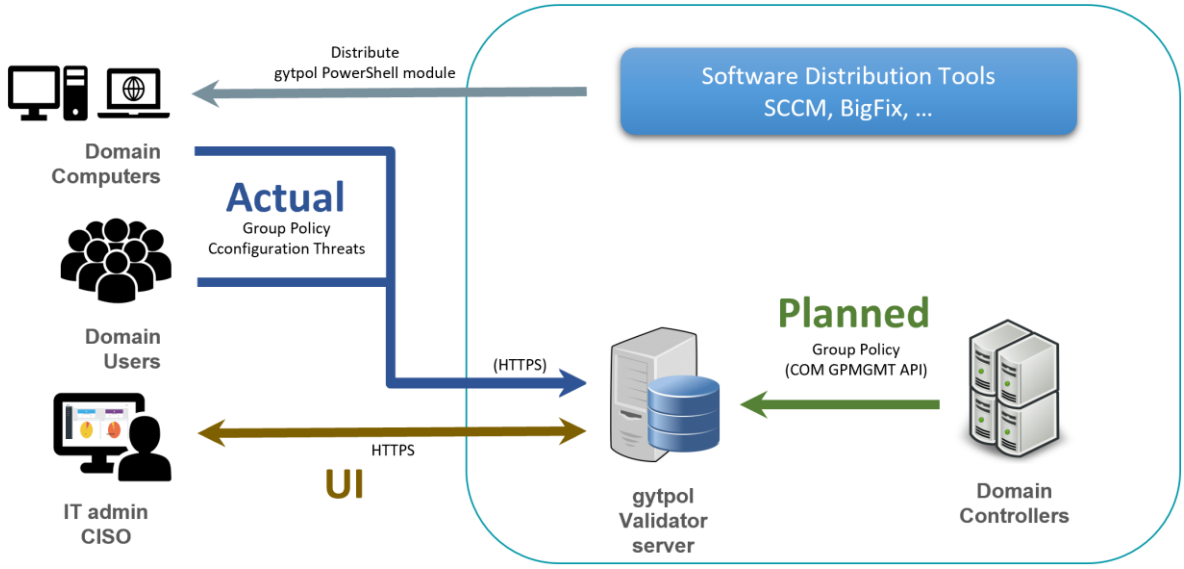


Figure 2. gytpol Validator Data Flow

Once deployed, gytpol Client installer creates a Windows Task on an endpoint running the associated signed PowerShell script. This script is triggered by user login, computer start-up or a predefined time period passed.

The main gytpol Validator data flow takes the following steps:

1. gytpol Client runs and sends; actually applied Group Policy, found threats and host information data to gytpol Server
2. upon receiving data from a gytpol Client, the gytpol Server retrieves expected (aka. planning) Group Policy from one of the specified domain controllers.
3. gytpol Server process and aggregates actual and expected data
4. IT and Security teams review the finding using Web UI
5. gytpol Server sends certain events to a SIEM system such as MicroFocus ArcSight, IBM QRadar or Splunk.

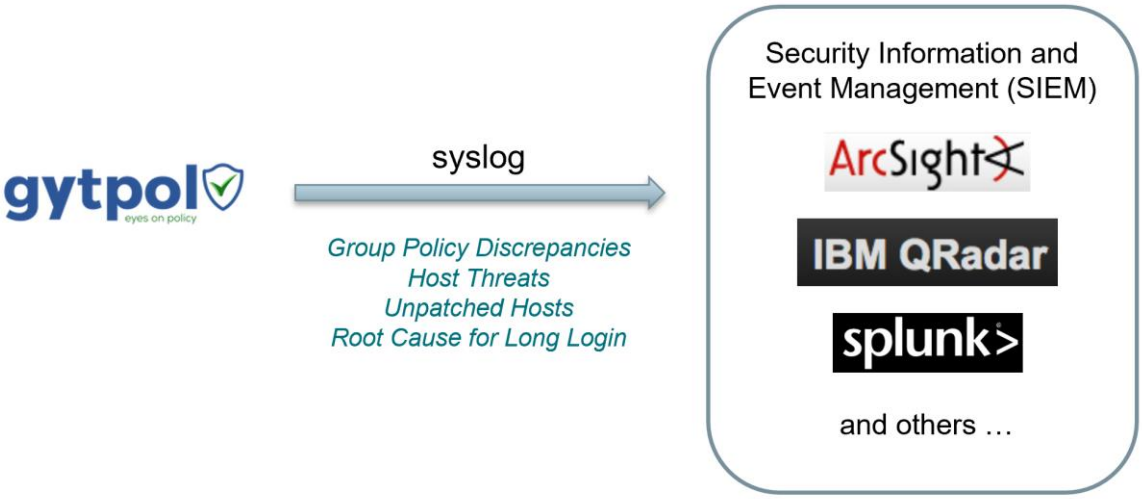


Figure 3. gytpol Validator SIEM Integration

gytpol Client

The gytpol Client is a lightweight signed PowerShell script that runs on endpoints as a Windows Task triggered by the following events:

- User login
- Computer start-up
- Security events triggered
- Specific time period passed with no other events triggered

When triggered by a user login, the gytpol Client runs in the context of the Windows domain user logged into the current computer. When triggered by a computer start-up, the gytpol Client runs in the context of the current Windows computer.

At each run, the gytpol Client collects the following information:

- Actually deployed Group Policy on the given computer (or user on computer). The client retrieves the actual Group Policy using the gpresult Microsoft Windows command.
- Host information including OS, environment variables, hardware, IP addresses, etc.
- Security vulnerabilities caused by misconfiguration of OS and 3rd party application - this is based on proprietary gytpol Client capabilities
- Version number of the gytpol Client itself
- Any errors that prevents the gytpol Client to retrieve required information

After collecting all the required information, the gytpol Client packages all the data in a zip file and sends it to gytpol Server over the HTTPS protocol.

gytpol Server

The gytpol Server collects data sent by gytpol Clients, retrieves related Planning definitions from the Domain Controllers, compares actually deployed Group Policies to what is expected by the Group Policy management tools, aggregates the results and presents to IT and Security users in an intuitive and interactive Web user interface.

Components

As shown in the Figure 4. below, the gytpol Server is implemented mostly as a set of .NET and Node.js microservices interacting with each other through HTTP based REST APIs. Most of gytpol Server components (i.e. microservices) are deployed as Windows Services allowing granular control over user permissions under with these microservices run.

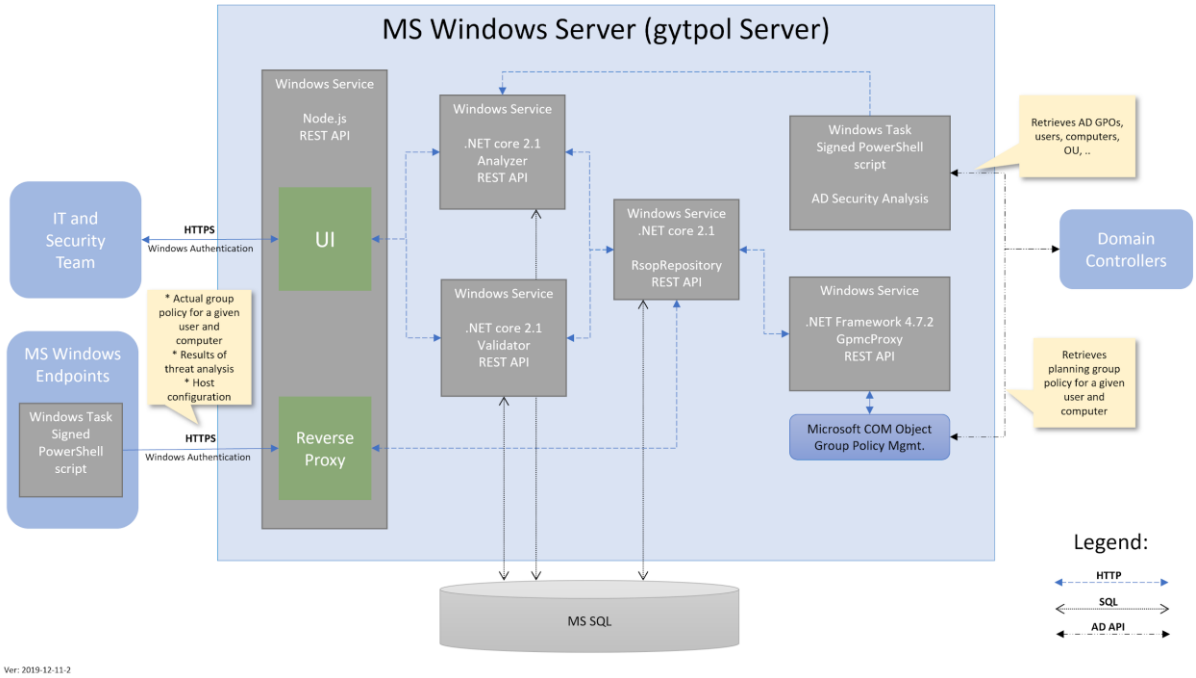


Figure 4. gytpol Server Architecture

The functional role and deployment details of each microservice are listed below.

Component	Platform	Port	Runs As	Role
UI	Node.js	9093	Windows Service	React.js UI
Reverse Proxy	Node.js	9093	Windows Service	Detach microservices
Validator	.NET core	8080	Windows Service	Group Policy threats
Analyzer	.NET core	8083	Windows Service	Other config threats
RsopRepository	.NET core	8082	Windows Service	Intermediate Repo
GpmcProxy	.NET framework	5000	Windows Service	Retrieve GP from DC
AD Security Analysis	PowerShell		Windows Task	Retrieve AD data

Database

Validator, Analyzer and RsopRepository store data in a MS SQL database. The exact MS SQL connection string is being configured during the product installation in the **appsettings.json** file.

The above microservices are automatically created (and upgrade when required) in the underlying databases using the provided connection string.

The following databases are created on the MS SQL server:

Validator - gytpol_validator, gytpol_profiler, gytpol_job_scheduler
Analyzer - gytpol_analyzer
RsopRepository - gytpol_rsop_reports

Troubleshooting

The gytpol Server components report errors into MS Windows Event Log under the following Sources:

- Gytpol Validator
- Gytpol RsopRepository
- Gytpol Analyzer
- Gytpol GpmcProxy
- Gytpol Security

Event log messages are self-descriptive and provide essential information for you, gytpol partner or gytpol own technical support team to address an issue.

License

The gytpol Validator product needs a valid **license.key** file to run. A gytpol customer receives this file from gytpol or a gytpol partner for the paid subscription period or for the period of a POC (i.e. proof of concept). The license imposes constraints on: number of users, number of computers, domain name, end date, the specific computer for which the *license.key* had been generated.

UI Authentication

The gytpol User Interface is a web UI, connecting through HTTPS port 9093 to the WebUI service running on the gytpol server. Furthermore, the user running the browser needs to be a Windows domain user with membership in the designated AD group selected for this purpose upon installation of the product and may further be configured later on.

Remote Employees Solution

Remote employees use computers owned by the employer to work from home, hotel, airport, etc. In many such cases an employee is not connected to the organizational network. Yet, organizations still want their endpoints to be secure. The gytpol Validator solution for Remote Employees address this use case.

As shown in Figure 5 below, the solution relies on the online service provided by gytpol. The service runs on the MS Azure public cloud infrastructure. It implements a secure pipeline delivering findings provided by the gytpol Client installed on the endpoint to the gytpol Server running on-prem.

The solution implements the following steps:

- gytpol Client is enabled for the Remote Employees Solution during installation
- gytpol Client runs conducts its scheduled analysis task
- gytpol Client identifies that the internal NW is not accessible
- gytpol Client sends the task results to the gytpol Online Service
- gytpol Online Service receives data sent by gytpol Clients
- gytpol Online Service keeps received data in the multitenant data store
- gytpol On-prem Server periodically pulls new data from gytpol Online Service
- gytpol Online Service sends data to gytpol On-prem Server
- gytpol On-prem Server stores the new data
- gytpol On-prem Server request gytpol On-prem Server to delete the new data
- gytpol Online Service deletes data upon a request from gytpol On-prem Server
- gytpol Online Service deletes remaining data upon Time-To-Live expiration

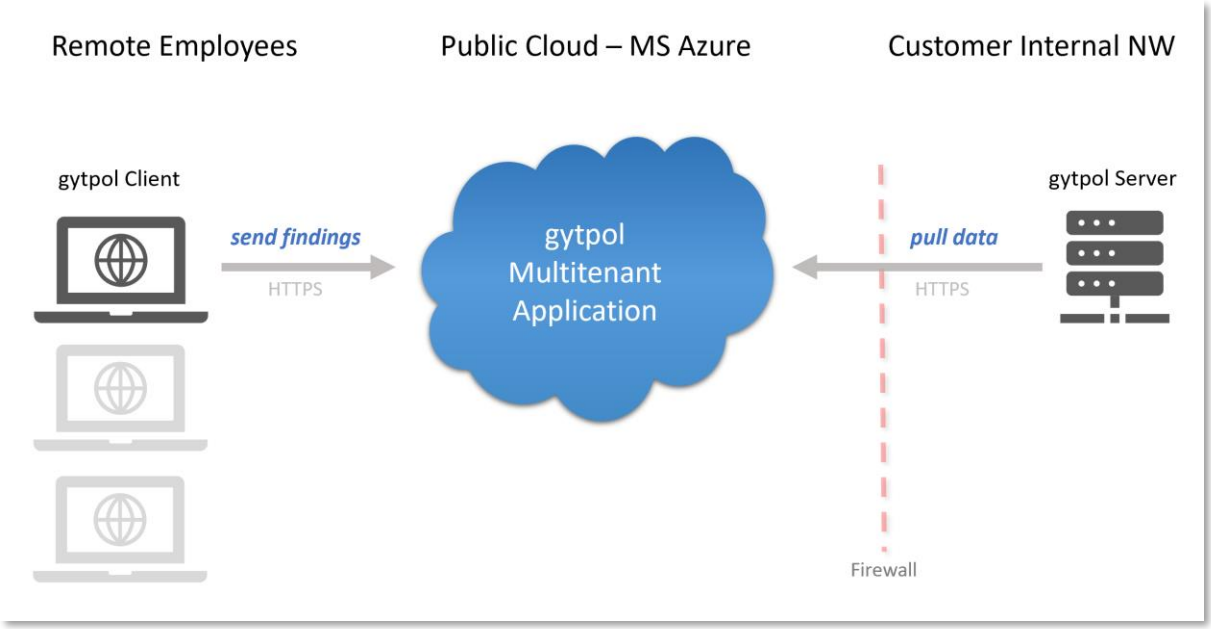


Figure 5. Remote Employees – Solution Architecture – End to End Encryption

Remediation

Please see gytpol Remediation document for details on the Remediation feature