GYTPOL Validator

Pre-Requisites Checker Tool Guide

Doc: GYT-TEC-004
Release: 08
Date: 15th May 2022

Confidential: GYTPOL and approved recipients

Total pages:	8

Doc. Title:	GYTPOL Validator Pre-Requisites Checker Tool Guide

Doc. No.:	GYT-TEC-004	**Classification:**	Confidential
Revision:	08	**Restriction:**	GYTPOL and approved recipients
Date:	15th May 2022	**Customer:**	

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

Introduction

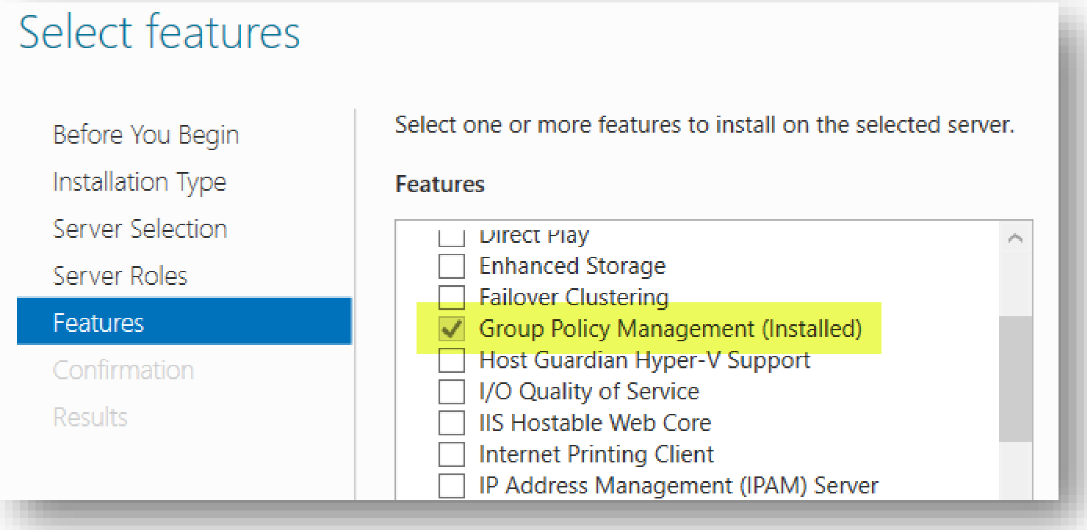
The purpose of this document is to provide a guide on how to download, install and use the Validator Pre-Requisites Checker Tool.

Pre-Requisites Checker

1. Download the Checker tool from the below link and copy it to the GYTPOL server: https://gytpolartifact.blob.core.windows.net/gytpolartifact/release/installer-prerequisite/latest/GytpolPrereq.exe?sp=r&st=2020-11-30T22:17:10Z&se=2022-11-01T06:17:10Z&spr=https&sv=2019-12-12&sr=b&sig=FBQ5oMiQ6ByqxDeM91RT3EuFTtLaP6TYT65EvvOuPic%3D

2. Open Server Manager on GYTPOL server → “Add Roles and Features” → click next until you get the **Features** tab:

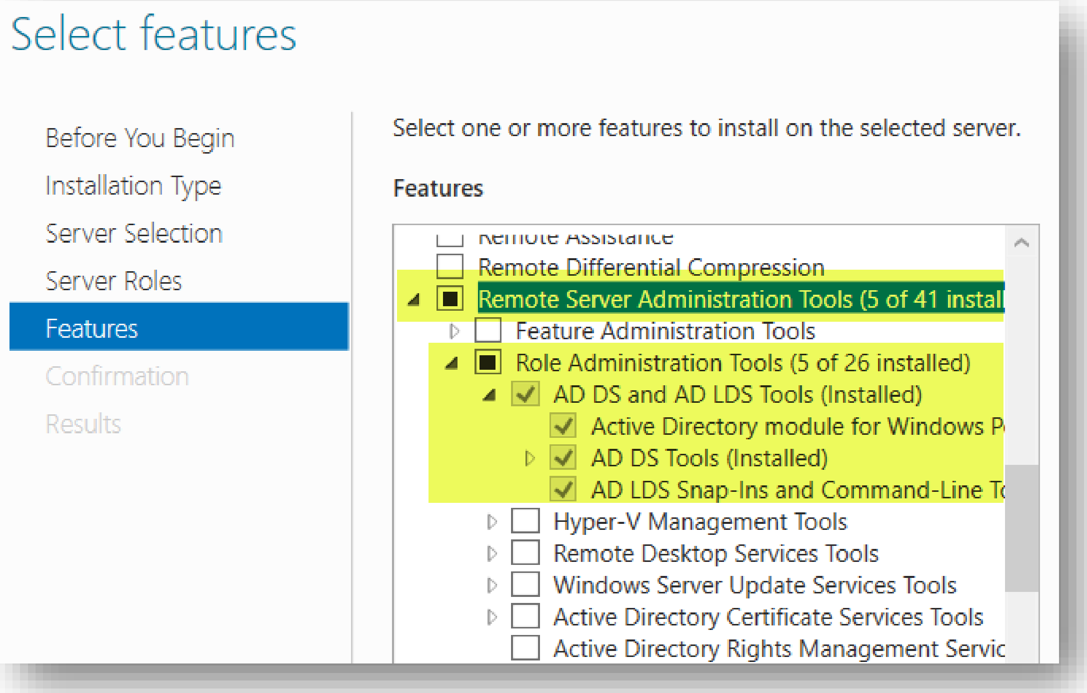
3. Check the following Features:
    a. **Group Policy Management**
    b. **Remote Server Administration Tools**
        i. Remote role Administrator Tools
            1. Active Directory module for PS
            2. AD DS Tools
            3. AD LDS Snap-Ins and Command-Line Tools



Select one or more features to install on the selected server.

Features

□ Direct Play
□ Enhanced Storage
□ Failover Clustering
☑ Group Policy Management (Installed)
□ Host Guardian Hyper-V Support
□ I/O Quality of Service
□ IIS Hostable Web Core
□ Internet Printing Client
□ IP Address Management (IPAM) Server



Select features

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

- □ Remote Assistance
- □ Remote Differential Compression
- ■ Remote Server Administration Tools (5 of 41 install
  - □ Feature Administration Tools
  - ■ Role Administration Tools (5 of 26 installed)
    - ☑ AD DS and AD LDS Tools (Installed)
      - ☑ Active Directory module for Windows P
      - ☑ AD DS Tools (Installed)
      - ☑ AD LDS Snap-Ins and Command-Line T
    - □ Hyper-V Management Tools
    - □ Remote Desktop Services Tools
    - □ Windows Server Update Services Tools
    - □ Active Directory Certificate Services Tools
    - □ Active Directory Rights Management Servic

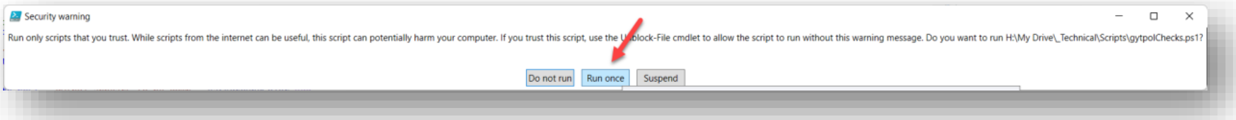
4. Click Next and Install and wait until it ends.

5. Please open **Windows Powershell ISE → Run as Adminstrator** and paste the following code:

```
cls
#set tls 1.2:
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

# check connectivity to Azure-EUROPE:
write-host "checking cloud connectivity:" -BackgroundColor Magenta
$gytEurope = (Invoke-WebRequest -URI "https://gytpol-cloud-
api.azurewebsites.net/api/v1.0/health_check").StatusDescription
if ($gytEurope -eq 'OK') {
        write-host "Europe connectivity passed: $gytEurope" -BackgroundColor Green
}
else {
        write-host "Europe connectivity failed: $gytEurope" -BackgroundColor Red
}

# check connectivity to Azure-USA:
$gytUSA = (Invoke-WebRequest -URI "https://gytpol-cloud-api-us-
func.azurewebsites.net/api/v1.0/health_check").StatusDescription
if ($gytUSA -eq 'OK') {
        write-host "USA connectivity passed: $gytUSA" -BackgroundColor Green
}
else {
        write-host "USA connectivity failed: $gytUSA" -BackgroundColor Red
}

# test ping _gytpol
write-host "checking _gytpol connectivity:" -BackgroundColor Magenta
$ping = (Test-NetConnection _gytpol).PingSucceeded
if ($ping) {
        write-host "_gytpol resolved and alive" -BackgroundColor Green
}
else {
        write-host "_gytpol appears to be down" -BackgroundColor Red
}

#print the host FQDN
write-host "Servers FQDN is" $env:COMPUTERNAME"."$env:USERDNSDOMAIN

#in case of FW open
$fwState = (Get-NetFirewallProfile -Name Domain).Enabled
if ($fwState) {
    $inboundRules = Get-NetFirewallRule -Direction Inbound | Where-Object
{$_.Enabled -eq 'True'}
        #$inboundPorts = $inboundRules | Get-NetFirewallPortFilter | Where-Object
{$_.LocalPort -like "909*"} | Select-Object -Property
InstanceID,Protocol,LocalPort,RemotePort
        $inboundPorts = $inboundRules | Get-NetFirewallPortFilter | Where-Object
{$_.LocalPort -like "909*"} | Select-Object -ExpandProperty LocalPort
        if ($null -ne $inboundPorts) {
                foreach ($rule in $inboundPorts) {
                        write-host "Rule $rule found"
                }
        } else {
                write-host "FW is Active but no Gytpol Rules were created on the
Domain FW" -BackgroundColor Red
        }
}
else {
        write-host "Windows Firewall is Disabled" -BackgroundColor Green
}

#test task creds:
$taskCreds = Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -
Name disabledomaincreds -ErrorAction Stop | Select-Object -ExpandProperty
disabledomaincreds
if ($taskCreds -eq 0) {
        write-host " Network access: OK" -BackgroundColor Green
} else {
        write-host "Network access: Do not allow storage of passwords and
credentials for network authentication is Enabled" -BackgroundColor Red
}
```

Click Run Script (F5) and see the results.

Note: If you have a security warning, please click **Run once**.



Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run H:\My Drive_Technical\Scripts\gytpolChecks.ps1?

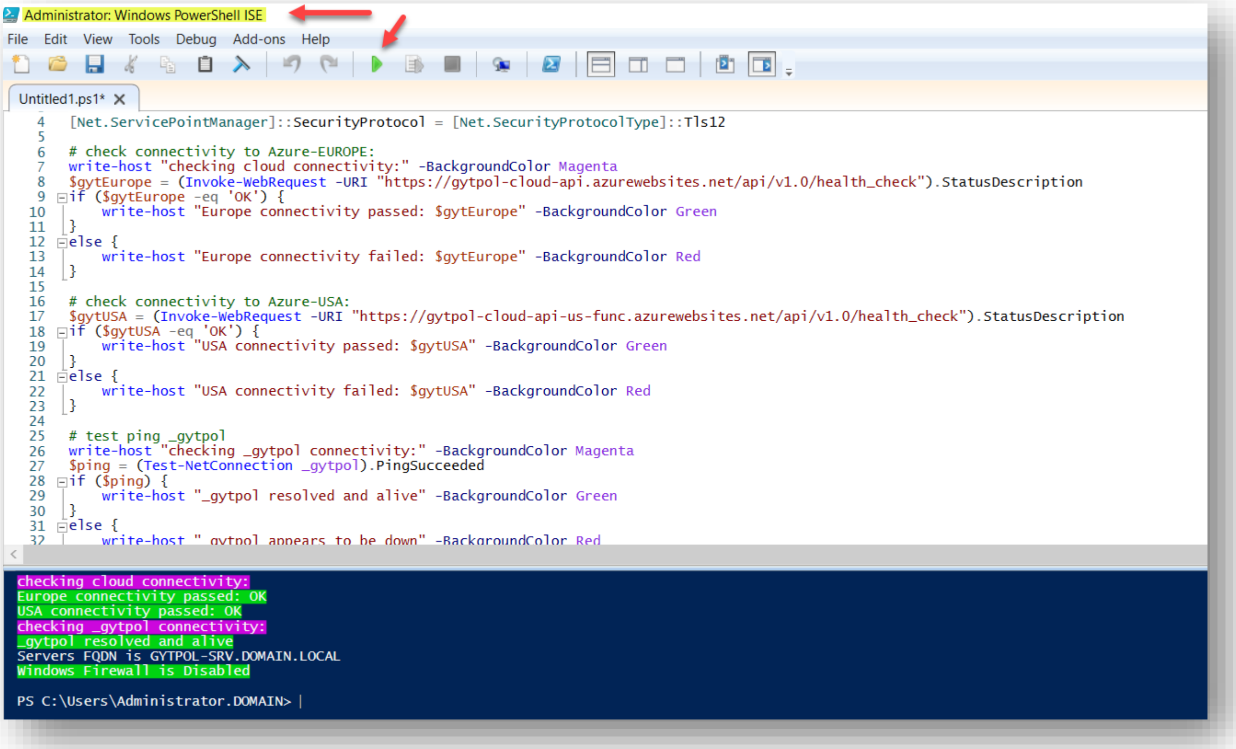
a. For customer with Remote Employees features, make sure that USA or Non-USA connectivity passed: OK.

b. **_gytpol** (CNAME record) is resolved and alive.

c. You can see your servers FQDN.

d. Your Windows Firewall is disabled

In case the Windows firewall is ON, please make see the ports 9090 and 9093 are found and shown. Otherwise, please set it according the System Requirements document.

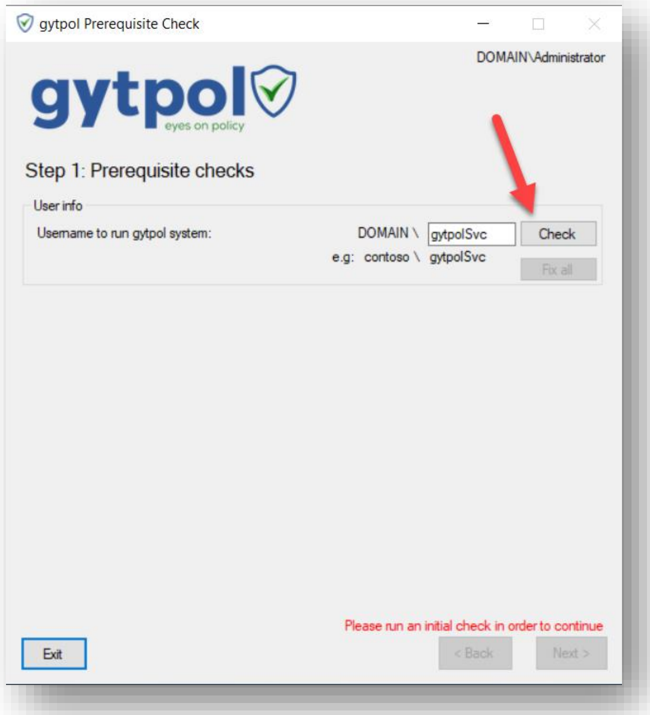


```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

# check connectivity to Azure-EUROPE:
write-host "checking cloud connectivity:" -BackgroundColor Magenta
$gytEurope = (Invoke-WebRequest -URI "https://gytpol-cloud-api.azurewebsites.net/api/v1.0/health_check").StatusDescription
if ($gytEurope -eq 'OK') {
    write-host "Europe connectivity passed: $gytEurope" -BackgroundColor Green
}
else {
    write-host "Europe connectivity failed: $gytEurope" -BackgroundColor Red
}

# check connectivity to Azure-USA:
$gytUSA = (Invoke-WebRequest -URI "https://gytpol-cloud-api-us-func.azurewebsites.net/api/v1.0/health_check").StatusDescription
if ($gytUSA -eq 'OK') {
    write-host "USA connectivity passed: $gytUSA" -BackgroundColor Green
}
else {
    write-host "USA connectivity failed: $gytUSA" -BackgroundColor Red
}

# test ping _gytpol
write-host "checking _gytpol connectivity:" -BackgroundColor Magenta
$ping = (Test-NetConnection _gytpol).PingSucceeded
if ($ping) {
    write-host "_gytpol resolved and alive" -BackgroundColor Green
}
else {
    write-host "_gytpol appears to be down" -BackgroundColor Red
```

```
checking cloud connectivity:
Europe connectivity passed: OK
USA connectivity passed: OK
checking _gytpol connectivity:
_gytpol resolved and alive
Servers FQDN is GYTPOL-SRV.DOMAIN.LOCAL
Windows Firewall is Disabled

PS C:\Users\Administrator.DOMAIN> |
```

6. Right click on the gytpol tool you downloaded in step 1 → **Run as Administrator** to start the Checker tool.

7. Enter the GYTPOL user i.e DOMAIN\gytpolSvc and press “Check”:



DOMAIN\Administrator

Step 1: Prerequisite checks

User info

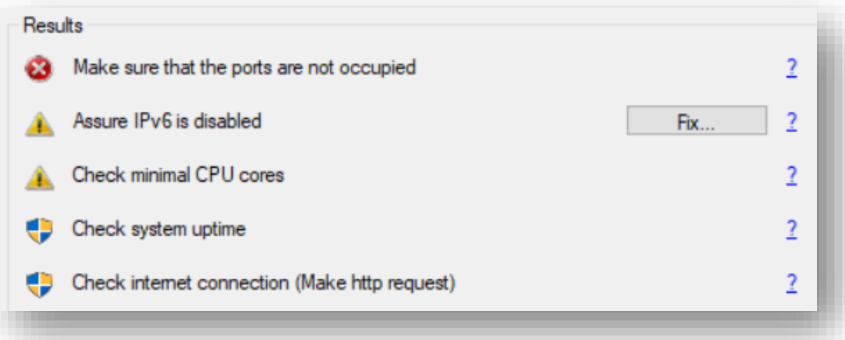
Username to run gytpol system: DOMAIN \ gytpolSvc

e.g: contoso \ gytpolSvc

Please run an initial check in order to continue

8. The checks will run for 1-2 minutes.
   The checklist contains: Internal ports, DC communication ports, User permissions, DNS CName record and other features are set correctly.

9. Wait to see the results:



Results

☒ Make sure that the ports are not occupied

⚠ Assure IPv6 is disabled

⚠ Check minimal CPU cores

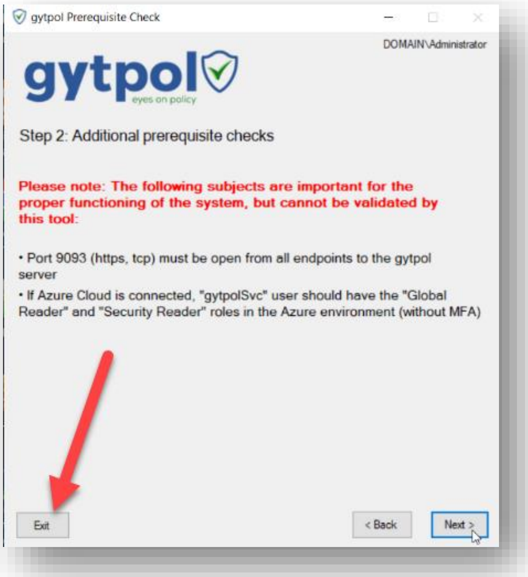
🛡 Check system uptime

🛡 Check internet connection (Make http request)

   a. Red X sign (error) – an error you should fix prior the installation.
      Note: Hover the mouse on the question mark (?) and see what’s need to be done.
   b. Yellow Exclamation mark (warning) - the check failed but it is not critical to fix it in order to continue the installation.
   c. Defender icon – check passed.

10. Once all is set and fixed, please click **Next**.
11. In "Additional prerequisite check" screen, please verify the port **9093** is open in your firewall from your endpoints and servers to GYTPOL server. If Azure connection is needed, please follow the prerequisites document.

12. Click Exit (**not Next**).



Step 2: Additional prerequisite checks

Please note: The following subjects are important for the proper functioning of the system, but cannot be validated by this tool:

• Port 9093 (https, tcp) must be open from all endpoints to the gytpol server

• If Azure Cloud is connected, "gytpolSvc" user should have the "Global Reader" and "Security Reader" roles in the Azure environment (without MFA)

13. Please restart the server before the installation.